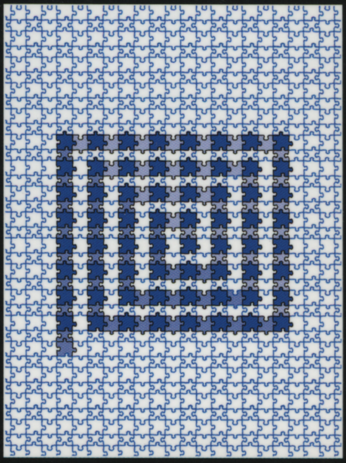
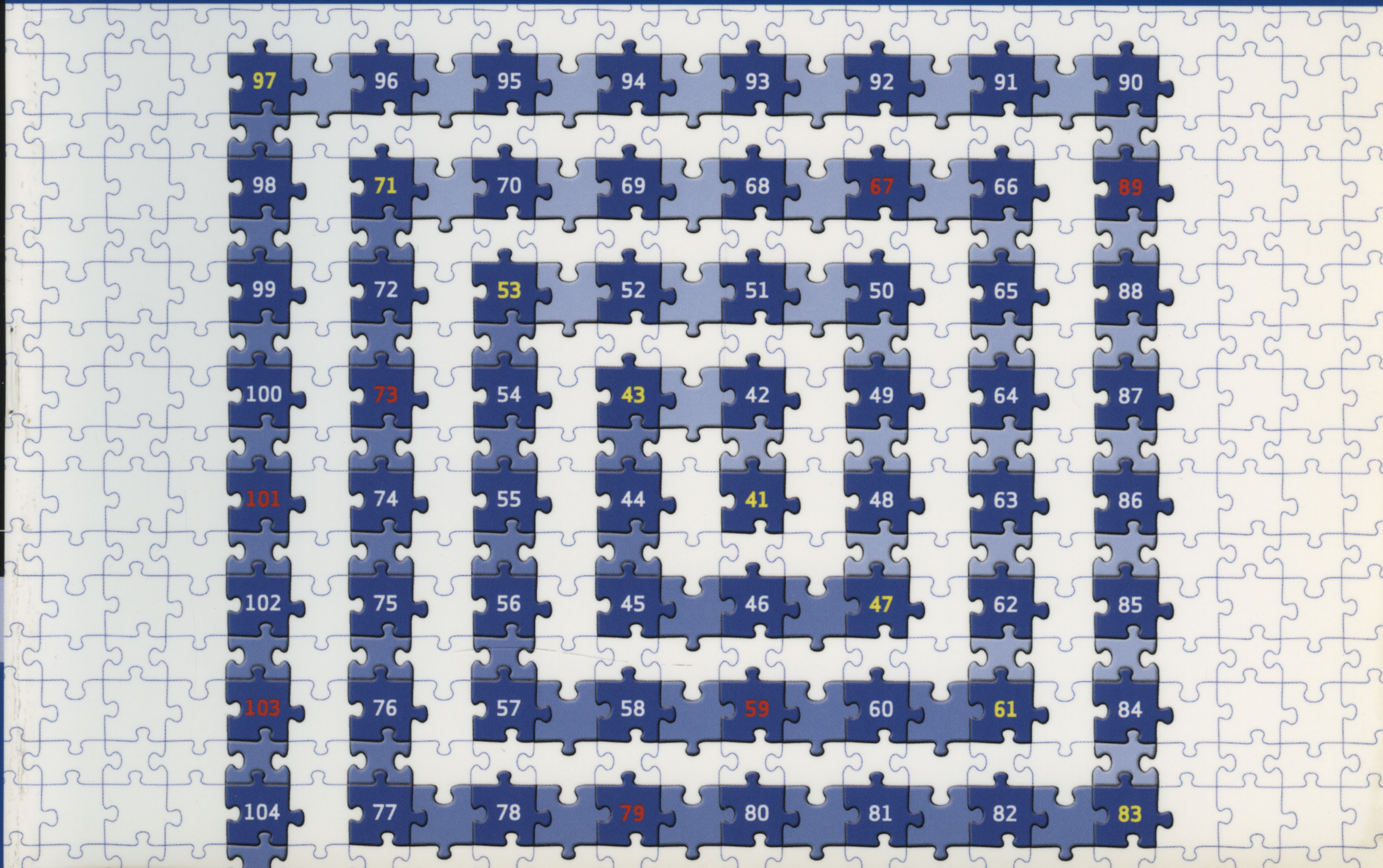
The Open University

M381 Number Theory and
Mathematical Logic



Number Theory **Unit 6**

Quadratic Reciprocity


97 96 95 94 93 92 91 90
98 71 70 69 68 67 66 89
99 72 53 52 51 50 65 88
100 73 54 43 42 49 64 87
101 74 55 44 41 48 63 86
102 75 56 45 46 47 62 85
103 76 57 58 59 60 61 84
104 77 78 79 80 81 82 83

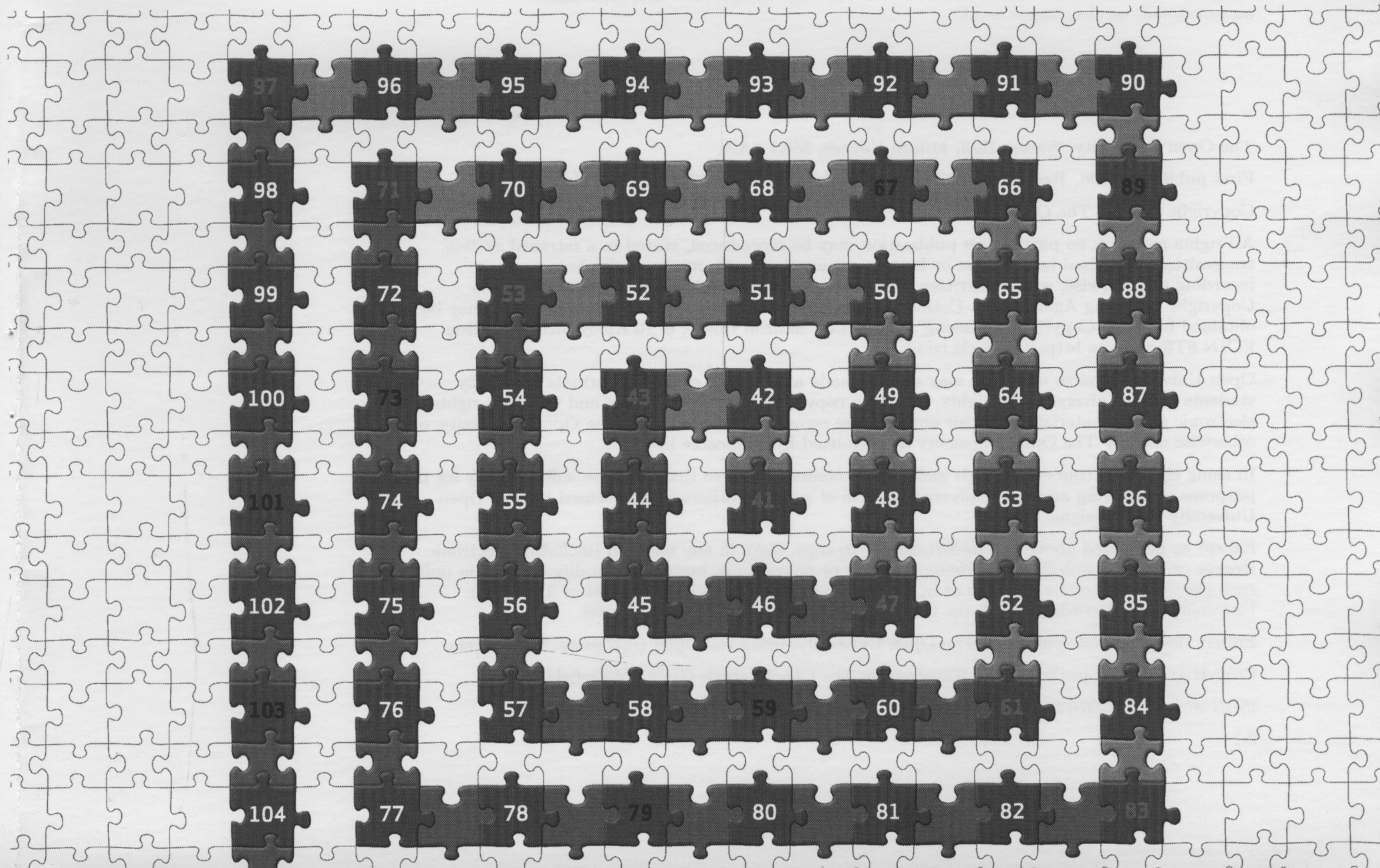
The Open University

M381 Number Theory and
Mathematical Logic

Number Theory **Unit 6**

Quadratic Reciprocity

Prepared for the Course Team by Alan Best


97
96
95
94
93
92
91
90
98
71
70
69
68
67
66
89
99
72
53
52
51
50
65
88
100
73
54
43
42
49
64
87
101
74
55
44
41
48
63
86
102
75
56
45
46
47
62
85
103
76
57
58
59
60
61
84
104
77
78
79
80
81
82
83

The M381 Number Theory Course Team

The Number Theory half of the course was produced by the following team:

Alan Best	*Author*
Andrew Brown	*Course Team Chair* and *Academic Editor*
Roberta Cheriyan	*Course Manager*
Bob Coates	*Critical Reader*
Dick Crabbe	*Publishing Editor*
Janis Gilbert	*Graphic Artist*
Derek Goldrei	*Critical Reader*
Caroline Husher	*Graphic Designer*
John Taylor	*Graphic Artist*

with valuable assistance from:

CMPU	*Mathematics and Computing, Course Materials Production Unit*
John Bayliss	*Reader*
Elizabeth Best	*Reader*
Jeremy Gray	*History Reader*
Alison Neil	*Reader*

The external assessor was:

Alex Wilkie	*Reader in Mathematical Logic, University of Oxford*

This publication forms part of an Open University course. Details of this and other Open University courses can be obtained from the Student Registration and Enquiry Service, The Open University, PO Box 197, Milton Keynes, MK7 6BJ, United Kingdom: tel. +44 (0)870 300 6090, e-mail general-enquiries@open.ac.uk

Alternatively, you may visit the Open University website at http://www.open.ac.uk where you can learn more about the wide range of courses and packs offered at all levels by The Open University.

To purchase a selection of Open University course materials, visit http://www.ouw.co.uk, or contact Open University Worldwide, Michael Young Building, Walton Hall, Milton Keynes, MK7 6AA, United Kingdom, for a brochure: tel. +44 (0)1908 858793, fax +44 (0)1908 858787, e-mail ouw-customer-services@open.ac.uk

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 1996. Reprinted 1997 and 2001. New edition 2007 with corrections.

Copyright © 1996 The Open University

All rights reserved; no part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC1N 8TS; website http://www.cla.co.uk.

Open University course materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic course materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic course materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or re-transmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using the Open University TEX System.

Printed and bound in the United Kingdom by The Charlesworth Group, Wakefield.

ISBN 978 0 7492 2276 5

2.1

CONTENTS

Introduction 4

1 Euler's Criterion 4
- 1.1 Quadratic residues 4
- 1.2 Euler's Criterion 7
- 1.3 Uses of Euler's Criterion 9

2 The Legendre Symbol 11
- 2.1 Properties of the Legendre symbol 11
- 2.2 Applications using the Legendre symbol 13

3 Gauss' Lemma 15
- 3.1 Proof of Gauss' Lemma 15
- 3.2 Applications of Gauss' Lemma 17
- 3.3 More cases of Dirichlet's Theorem 19

4 The Law of Quadratic Reciprocity 21
- 4.1 Understanding the law 21
- 4.2 Proof of LQR 23
- 4.3 Applications of LQR 26

Additional Exercises 28

Solutions to the Problems 30

Solutions to Additional Exercises 37

Index 43

INTRODUCTION

In *Unit 4* we studied polynomial congruences. We found that, provided we take congruence to a prime modulus, a polynomial congruence of degree k has at most k incongruent solutions. In this respect polynomial congruences are similar to polynomial equations. In this unit we are going to concentrate on polynomial congruences of degree 2, called *quadratic congruences.* We shall quickly discover that the key problem is to solve the congruence

$$x^2 \equiv a \pmod{p}.$$

In most cases the modulus will be an odd prime.

In other words we shall try to find which integers are squares modulo p. In previous units we have solved such problems for small primes p. For instance, by working out 0^2, 1^2, 2^2, 3^2 and 4^2 modulo 5 we see that the only squares modulo 5 are 0, 1 and 4. It follows that the quadratic congruences

$$x^2 \equiv 2 \pmod{5} \text{ and } x^2 \equiv 3 \pmod{5}$$

are each unsolvable.

As the task of solving quadratic equations presents little challenge, the thought of devoting a whole unit to quadratic congruences might, understandably, seem unexciting. Be patient! Investigation of when a quadratic congruence has solutions (without actually solving it) leads us through three classic results of number theory: Euler's Criterion, Gauss' Lemma and the Law of Quadratic Reciprocity. The latter is a most fascinating result, described by Gauss as the 'gem of higher arithmetic'. The consequences of these results are far-reaching in other areas of number theory. In this unit we shall use them to establish several more special cases of Dirichlet's Theorem on primes in arithmetic progressions, which we first investigated in *Unit 2.* Later in the course we shall see further applications of these results to the solution of Diophantine equations, which are the subject of *Unit 8.*

1 EULER'S CRITERION

1.1 Quadratic residues

Consider the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

where p is an odd prime and $a \not\equiv 0 \pmod{p}$. In an attempt to solve this congruence we can write the left-hand side in an alternative form by 'completing the square' to get all involvement of x into a single squared term. To achieve that, we first multiply through by $4a$, which will not affect the solutions since $\gcd(4a, p) = 1$:

$a \not\equiv 0 \pmod{p} \iff \gcd(a,p) = 1$
$\iff p$ does not divide a.

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}.$$

That is,

$$(2ax + b)^2 + 4ac - b^2 \equiv 0 \pmod{p},$$

This is essentially the process used to obtain the 'quadratic formula'

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

and adding $b^2 - 4ac$ to both sides,

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}.$$

If we now let $d = b^2 - 4ac$ and put $y = 2ax + b$ the quadratic congruence takes the simplified form

$$y^2 \equiv d \pmod{p}.$$

For each solution y_0 of this congruence we can recover a solution of the original congruence by solving $2ax + b \equiv y_0 \pmod{p}$, which is known to be uniquely solvable since $\gcd(2a, p) = 1$.

To illustrate this let us work through a specific example.

Example 1.1

Solve $2x^2 + 2x + 1 \equiv 0 \pmod{29}$.

We begin by multiplying through by $4 \times 2 = 8$:

$$16x^2 + 16x + 8 \equiv 0 \pmod{29},$$

and then complete the square:

$$(4x + 2)^2 + 4 \equiv 0 \pmod{29}.$$

Now add -4 to both sides:

$$(4x + 2)^2 \equiv -4 \pmod{29}.$$

Putting $y = 4x + 2$, and replacing -4 by the congruent integer 25 we arrive at

$$y^2 \equiv 25 \pmod{29},$$

which has the two solutions

$$y \equiv 5 \pmod{29} \quad \text{and} \quad y \equiv -5 \pmod{29}.$$

Lagrange's Theorem guarantees that there are no more than these two.

The solutions in x are therefore obtained by solving two linear congruences:

$$\begin{aligned} 4x + 2 \equiv 5 \pmod{29} &\iff 4x \equiv 3 \equiv 32 \pmod{29} \\ &\iff x \equiv 8 \pmod{29}; \\ 4x + 2 \equiv -5 \pmod{29} &\iff 4x \equiv -7 \equiv -36 \pmod{29} \\ &\iff x \equiv -9 \equiv 20 \pmod{29}. \end{aligned}$$

So the two solutions are $x \equiv 8, 20 \pmod{29}$.

◆

The solutions obtained can, of course, be checked by substituting 8 and 20 back into the original congruence.

Problem 1.1

Solve the following quadratic congruences using the process illustrated in Example 1.1.

(a) $5x^2 + 7x + 1 \equiv 0 \pmod{13}$

(b) $x^2 + x + 1 \equiv 0 \pmod{5}$

(c) $x^2 + 3x + 4 \equiv 0 \pmod{7}$

The examples in Problem 1.1 show that a quadratic congruence to prime modulus may have 0, 1 or 2 solutions. They also pinpoint what is the key issue in solving $ax^2 + bx + c \equiv 0 \pmod{p}$. This congruence has solution(s) if, and only if, $b^2 - 4ac$ is congruent modulo p to a square. What we need is a way of determining which integers are the squares modulo p. First we introduce some new terminology.

The number $b^2 - 4ac$ is called the *discriminant* of the quadratic $ax^2 + bx + c$.

Definition 1.1 Quadratic residues

Let p be an odd prime and $a \not\equiv 0 \pmod{p}$. If the congruence $x^2 \equiv a \pmod{p}$ has a solution then a is said to be a *quadratic residue* of p. Otherwise a is a *quadratic non-residue* of p. We refer to whether a is a quadratic residue or quadratic non-residue of p as being the *quadratic character* of a modulo p.

Notice that if $a \equiv b \pmod{p}$ then the congruence $x^2 \equiv a \pmod{p}$ has a solution if, and only if, the congruence $x^2 \equiv b \pmod{p}$ has a solution, and so congruent integers are of the same quadratic character, that is, both are quadratic residues of p or both are quadratic non-residues of p. For this reason it will be enough to consider the quadratic character of the non-zero least positive residues modulo p. So when, as in the coming example, we ask for the quadratic residues or non-residues of p, the expected answer will be a collection of integers in the range from 1 to $p-1$.

Example 1.2

Find the quadratic residues and the quadratic non-residues of 11.

To list the quadratic residues of 11 it suffices to determine the squares $1^2, 2^2, \ldots, 10^2$ modulo 11.

$$\begin{aligned}
1^2 &\equiv 1 \pmod{11}\\
2^2 &\equiv 4 \pmod{11}\\
3^2 &\equiv 9 \pmod{11}\\
4^2 &\equiv 5 \pmod{11}\\
5^2 &\equiv 3 \pmod{11}\\
6^2 &\equiv (-5)^2 \equiv 3 \pmod{11}\\
7^2 &\equiv (-4)^2 \equiv 5 \pmod{11}\\
8^2 &\equiv (-3)^2 \equiv 9 \pmod{11}\\
9^2 &\equiv (-2)^2 \equiv 4 \pmod{11}\\
10^2 &\equiv (-1)^2 \equiv 1 \pmod{11}
\end{aligned}$$

Therefore the quadratic residues of 11 are 1, 3, 4, 5 and 9. The quadratic non-residues of 11 are the remaining non-zero least positive residues, namely 2, 6, 7, 8 and 10. ◆

Problem 1.2

Determine the quadratic residues and the quadratic non-residues of 13. Hence determine the values of c for which the congruence $x^2 + x - c \equiv 0 \pmod{13}$ has solutions.

You may have noticed that our definition excludes 0 as a quadratic residue despite the fact that 0 is certainly a square. We also removed from consideration the case $p = 2$, where the only non-zero residue, 1, is a square. The major reason is that these decisions enable us to express results in neater forms. For example, the congruence

$$x^2 \equiv a \pmod{p}$$

has no solutions if a is a quadratic non-residue of p, has one solution if $a \equiv 0 \pmod{p}$ and two solutions if a is a quadratic residue of p. In addition, with these definitions, as we have seen for the examples $p = 11$ and $p = 13$, there are the same number of quadratic residues as there are quadratic non-residues. We establish this fact now.

If $x \equiv b \pmod{p}$ is a solution then so too is $x \equiv -b \pmod{p}$ and $b \not\equiv -b \pmod{p}$ except when $b \equiv 0 \pmod{p}$.

Theorem 1.1 The quadratic residues of p

For any odd prime p there are $\dfrac{p-1}{2}$ quadratic residues and $\dfrac{p-1}{2}$ quadratic non-residues. The quadratic residues are congruent modulo p to the integers $1^2, 2^2, 3^2, \ldots, \left(\dfrac{p-1}{2}\right)^2$.

Proof of Theorem 1.1

The quadratic residues of p are the integers which result from the evaluation of the squares $1^2, 2^2, 3^2, \ldots, (p-1)^2$ modulo p. But $r^2 = (-r)^2$ and so these $p-1$ integers fall into congruent pairs modulo p, namely

$$1^2 \equiv (p-1)^2,\ 2^2 \equiv (p-2)^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2 \equiv \left(\frac{p+1}{2}\right)^2$$

Notice that we require p to be odd here.

Therefore each quadratic residue of p is congruent to one of the $\frac{p-1}{2}$ integers $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

As $r^2 \not\equiv 0 \pmod{p}$, for $1 \le r < p$, the integer 0 is not listed amongst these.

To complete the proof it remains to show that no two of these integers are congruent modulo p. With that objective in mind suppose that

$$r^2 \equiv s^2 \pmod{p}\,, \text{ for some } 1 \le s \le r \le \frac{p-1}{2}.$$

Our goal is to deduce from this that $r = s$. Now $r^2 \equiv s^2 \pmod{p}$ means that p is a divisor of $r^2 - s^2$ or, after factorizing, p divides $(r-s)(r+s)$. Euclid's Lemma takes us a step further: either p divides $r-s$ or p divides $r+s$. The latter is impossible since $2 \le r+s \le p-1$. As to the former, the fact that $r-s$ lies in the range $0 \le r-s < \frac{p-1}{2}$ confirms that p can only divide $r-s$ when $r-s=0$; that is, when $r=s$.

Thus there are exactly $\frac{p-1}{2}$ quadratic residues and hence $\frac{p-1}{2}$ quadratic non-residues. ■

1.2 Euler's Criterion

We shall keep returning to the task of actually solving congruences, but for the time being we shall concentrate on the key question which confronts us when deciding whether or not a quadratic congruence has solutions.

> Given $a \not\equiv 0 \pmod{p}$, is a a quadratic residue of p?

Theorem 1.1 suggests one line of attack by providing a means of listing all the quadratic residues of p. However the amount of computation it entails, even for a relatively small prime p, forces us to look around for some alternative method. Our next result, first attributed to Euler, provides such an alternative method. Whilst it can still involve cumbersome computations it is a very useful theoretical result for which we shall find numerous applications.

Theorem 1.2 Euler's Criterion

Let p be an odd prime and $a \not\equiv 0 \pmod{p}$. Then a is a quadratic residue of p if, and only if, $a^{(p-1)/2} \equiv 1 \pmod{p}$ and is a quadratic non-residue of p if, and only if, $a^{(p-1)/2} \equiv -1 \pmod{p}$.

The proof that we are going to give of Euler's Criterion involves careful pairing of the integers forming the set of non-zero least positive residues modulo p. We shall first illustrate the line of proof for the case of the prime 13.

We have seen in Problem 1.2 that 2 is a quadratic non-residue of 13. Consider the congruence $bx \equiv 2 \pmod{13}$, where b is any of the integers $1, 2, \ldots, 12$. Since $\gcd(b, 13) = 1$ this congruence has a unique solution. The solution is certainly not $x \equiv 0 \pmod{13}$ and neither is it $x \equiv b \pmod{13}$, for then $b^2 \equiv 2 \pmod{13}$ which would contradict the fact that 2 is a quadratic non-residue. Hence, for each choice of b, the solution of $bx \equiv 2 \pmod{13}$ is

We take the slightly easier case of a non-residue first.

one of the *other* integers in the set $\{1, 2, \ldots, 12\}$. It follows that these 12 integers break into pairs whose product is congruent modulo 13 to 2. These pairs are as follows.

$$\begin{array}{ll} 1 \times 2 \equiv 2 \pmod{13} & 3 \times 5 \equiv 2 \pmod{13} \\ 4 \times 7 \equiv 2 \pmod{13} & 6 \times 9 \equiv 2 \pmod{13} \\ 8 \times 10 \equiv 2 \pmod{13} & 11 \times 12 \equiv 2 \pmod{13} \end{array}$$

Multiplying these six congruences together we obtain

$$12! \equiv 2^6 \pmod{13}.$$

But we know from Wilson's Theorem that $12! \equiv -1 \pmod{13}$, and so

$$2^6 \equiv -1 \pmod{13},$$

which is the claim of Euler's Criterion for the case of the quadratic non-residue 2 of 13.

There is nothing special here about the prime 13 nor of the chosen integer 2. The crux of the general proof which follows shortly is to show that, for any odd prime p and any quadratic non-residue a of p, the integers in the set $\{1, 2, \ldots, p-1\}$ break into pairs with product congruent modulo p to a.

To illustrate Euler's Criterion for the case of a quadratic residue we proceed in a similar vein. Take $a = 3$ and and consider solutions of $bx \equiv 3 \pmod{13}$. The difference this time is that the congruence $x^2 \equiv 3 \pmod{13}$ does have solutions, namely $x \equiv 4 \pmod{13}$ and $x \equiv 9 \pmod{13}$. The remaining ten integers in $\{1, 2, \ldots, 12\}$ break into pairs whose product is congruent modulo 13 to 3.

We discovered that 3 is a quadratic residue of 13 in Problem 1.2.

$$\begin{array}{ll} 1 \times 3 \equiv 3 \pmod{13} & 2 \times 8 \equiv 3 \pmod{13} \\ 5 \times 11 \equiv 3 \pmod{13} & 6 \times 7 \equiv 3 \pmod{13} \\ 10 \times 12 \equiv 3 \pmod{13} & \end{array}$$

If we multiply together the left-hand sides of these congruences the outcome will not be 12!, since the integers 4 and 9 are missing. To rectify this, so that we can subsequently appeal to Wilson's Theorem, we include the additional congruence whose left-hand side is 4×9:

$$4 \times 9 \equiv 36 \equiv -3 \pmod{13}.$$

(As we shall see shortly, it is no accident that the right-hand side of this congruence has turned out to be the negative of the quadratic residue under consideration.) Multiplying all six congruences together we reach

$$12! \equiv 3^5 \times (-3) \equiv -3^6 \pmod{13},$$

whereupon invocation of Wilson's Theorem leads to $3^6 \equiv 1 \pmod{13}$. This is what Euler's Criterion claims for the quadratic residue 3 of 13.

Our task now is to convert these illustrations into general arguments.

Proof of Euler's Criterion

Let a be a quadratic non-residue of p and let b be any integer in $\{1, 2, \ldots, p-1\}$. The linear congruence $bx \equiv a \pmod{p}$ has a unique solution b' also in $\{1, 2, \ldots, p-1\}$. Note that $b \neq b'$, for otherwise $b^2 \equiv a \pmod{p}$ and a would be a quadratic residue of p. It follows that the integers in $\{1, 2, \ldots, p-1\}$ fall into $\dfrac{p-1}{2}$ pairs b, b' with the property that $bb' \equiv a \pmod{p}$. Hence

$$(p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-1) \equiv a \times a \times \cdots \times a \equiv a^{(p-1)/2} \pmod{p}.$$

If we now bring in Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$, we reach

$$a^{(p-1)/2} \equiv -1 \pmod{p}, \text{ for any quadratic non-residue } a.$$

Let us now attempt the same argument for the case of a being a quadratic residue of p. This time the congruence $x^2 \equiv a \pmod{p}$ has a solution.

In fact it will have exactly two solutions. Lagrange's Theorem guarantees that it has at most two solutions and if c is one solution in $\{1, 2, \ldots, p-1\}$ then $p - c$ is certainly another since

$$(p-c)^2 \equiv (-c)^2 \equiv c^2 \equiv a \pmod{p}$$

and $c \neq p - c$ as $p = 2c$ is impossible.

If we remove c and $p - c$ from $\{1, 2, \ldots, p-1\}$ then, as before, the remaining integers fall into $\dfrac{p-3}{2}$ pairs b, b' with the property that $bb' \equiv a \pmod{p}$. So this time

$$\begin{aligned}(p-1)! &= 1 \times 2 \times \cdots \times c \times \cdots \times (p-c) \times \cdots \times (p-1) \\ &\equiv a \times a \times \cdots \times a \times c \times (p-c) \pmod{p} \\ &\equiv a^{(p-3)/2}(-c^2) \pmod{p} \\ &\equiv a^{(p-3)/2}(-a) \pmod{p} \\ &\equiv -a^{(p-1)/2} \pmod{p}.\end{aligned}$$

Replacing $(p-1)!$ by -1 and cancelling by -1 leads to

$$a^{(p-1)/2} \equiv 1 \pmod{p}, \quad \text{for any quadratic residue } a.$$

We have now shown that if a is a quadratic residue, then $a^{(p-1)/2} \equiv 1 \pmod{p}$ and if a is a quadratic non-residue, then $a^{(p-1)/2} \equiv -1 \pmod{p}$.

To complete the 'only if' parts suppose first that $a^{(p-1)/2} \equiv 1 \pmod{p}$. As $a \not\equiv 0 \pmod{p}$, it is either a quadratic residue or a quadratic non-residue. If we assume that a is a non-residue then $a^{(p-1)/2} \equiv -1 \pmod{p}$ and this would imply that $1 \equiv -1 \pmod{p}$ which is false for an odd prime. So if $a^{(p-1)/2} \equiv 1 \pmod{p}$ then a is a quadratic residue. The non-residue case follows similarly. ■

1.3 Uses of Euler's Criterion

We have already determined the quadratic residues of the prime 13 but there is no harm in tackling the same problem by a totally different method. As we shall see, Euler's Criterion is very useful for determining whether or not a given integer is a quadratic residue, but it is less helpful when we wish to determine all the quadratic residues of a given prime.

Example 1.3

Use Euler's Criterion to determine the quadratic residues and non-residues of the prime 13.

To determine whether or not a is a quadratic residue of 13, Euler's Criterion tells us to investigate $a^{(13-1)/2} = a^6$ in the certain knowledge that for any a in the set $\{1, 2, 3, \ldots, 12\}$ either $a^6 \equiv 1 \pmod{13}$, in which case a is a quadratic residue, or $a^6 \equiv -1 \pmod{13}$, in which case a is a quadratic non-residue.

$$\begin{aligned}&1^6 \equiv 1 \pmod{13} \\ &2^6 \equiv 16 \times 4 \equiv 12 \equiv -1 \pmod{13} \\ &3^6 \equiv 3^3 \times 3^3 \equiv 1 \times 1 \equiv 1 \pmod{13} \\ &4^6 \equiv (4^2)^3 \equiv 3^3 \equiv 1 \pmod{13} \\ &5^6 \equiv (5^2)^3 \equiv (-1)^3 \equiv -1 \pmod{13} \\ &6^6 \equiv (6^2)^3 \equiv (-3)^3 \equiv -1 \pmod{13}\end{aligned}$$

No further computation is needed because

$$(13-r)^6 \equiv (-r)^6 \equiv r^6 \pmod{13},$$

and so,

$$7^6 \equiv 6^6, 8^6 \equiv 5^6, 9^6 \equiv 4^6, 10^6 \equiv 3^6, 11^6 \equiv 2^6 \text{ and } 12^6 \equiv 1^6 \pmod{13}.$$

The list of quadratic residues of 13 is therefore 1, 3, 4, 9, 10 and 12 and the non-residues are the other six non-zero least positive residues, namely 2, 5, 6, 7, 8 and 11.

◆

Problem 1.3

Determine the quadratic character of 5 for each of the primes 11, 17 and 19.

Primitive roots provide an alternative way of determining the quadratic residues of an odd prime p. Suppose that r is a primitive root of p. Then the set of integers $\{r, r^2, \ldots, r^{p-1}\}$ is a reduced set of residues for p. That is, after replacing each by its least positive residue modulo p (and reordering as appropriate), it is the set $\{1, 2, \ldots, p-1\}$. Half of these integers are quadratic residues and the other half are quadratic non-residues, their designations being readily seen: the $\frac{p-1}{2}$ integers $\{r^2, r^4, \ldots, r^{p-1}\}$, being even powers of the primitive root and hence squares, are the quadratic residues.

In *Unit 5* we mentioned (without proof) that every prime does have a primitive root.

Example 1.4

Given that 2 is a primitive root of 19 determine the quadratic residues of 19.

The first $\frac{19-1}{2} = 9$ even powers of 2 give the quadratic residues of 19 whilst the remaining 9 non-zero integers less than 19 are the quadratic non-residues.

$$2^2 = 4$$
$$2^4 = 16$$
$$2^6 = 64 \equiv 7 \pmod{19}$$
$$2^8 \equiv 7 \times 4 \equiv 28 \equiv 9 \pmod{19}$$
$$2^{10} \equiv 9 \times 4 \equiv 36 \equiv 17 \pmod{19}$$
$$2^{12} \equiv 17 \times 4 \equiv 68 \equiv 11 \pmod{19}$$
$$2^{14} \equiv 11 \times 4 \equiv 44 \equiv 6 \pmod{19}$$
$$2^{16} \equiv 6 \times 4 \equiv 24 \equiv 5 \pmod{19}$$
$$2^{18} \equiv 5 \times 4 \equiv 1 \pmod{19}$$

In each case we multiply the previous value by 4 and reduce modulo 19.

The quadratic residues of 19 are therefore 1, 4, 5, 6, 7, 9, 11, 16 and 17.

◆

From the identity

$$(ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2}$$

and knowledge of the quadratic character of a and b, Euler's Criterion tells us immediately whether or not the product ab is a quadratic residue. For example, if a is a quadratic residue of p, so that $a^{(p-1)/2} \equiv 1 \pmod{p}$, and b is a quadratic non-residue of p, so that $b^{(p-1)/2} \equiv -1 \pmod{p}$, then multiplying the two together gives $(ab)^{(p-1)/2} \equiv -1 \pmod{p}$ showing that ab is a quadratic non-residue. Looking similarly at the other three combinations we obtain the following table, which is essentially determined by the products of 1 (for residue) and -1 (for non-residue).

Table 1.1 Table of residue multiplication

	residue	non-residue
residue	residue	non-residue
non-residue	non-residue	residue

You may wish to refer to this table in answering the following problems.

Problem 1.4

Let p be an odd prime.

(a) If $b \not\equiv 0 \pmod{p}$ and the congruence $ax^2 \equiv b \pmod{p}$ has a solution what can you deduce about the quadratic characters of a and b?

(b) If -1 is a quadratic residue of p what can you infer about p?

(c) If a is a quadratic residue of p under what circumstances is $p - a$ also a quadratic residue?

2 THE LEGENDRE SYMBOL

2.1 Properties of the Legendre symbol

Adrien-Marie Legendre (1752–1833)

Legendre was born in Toulouse and educated at the Mazarin College in Paris. Throughout a distinguished mathematical career Legendre contributed to significant advances in many fields. He was mainly an analyst, but arguably the finest of many books that he published was *Elements de Geometrie*, in which he reorganized the geometrical content of Euclid's *Elements* systematically, offering simpler, but equally rigorous proofs. The result was one of the most successful textbooks ever written; it was still being used as a standard text in school geometry until nearly the end of the nineteenth century.

Earlier Legendre had written a three volume comprehensive treatment of Integral Calculus, followed by a further three volume work on Elliptic Integrals. In these works he introduced numerous tools of analysis still used by applied mathematicians, including the beta and gamma functions and the Legendre polynomials, which are used in solving certain differential equations.

Legendre was not a great innovator in number theory but his writings did point mathematicians of the nineteenth century towards fruitful areas for investigation. In 1798 he published a two volume work, *Essai sur la theorie des nombres*, probably the first treatise devoted solely to number theory. An expanded edition, *Theorie des nombres*, was printed in 1830 and this included results from Legendre's work in the intervening years, work which had been inspired through correspondence with Gauss. Amongst many other results, he proved that the equation $x^5 + y^5 = z^5$ has no solution in positive integers — this is a particular case of Fermat's Last Theorem which we shall meet in the final unit of the course. On the question of distribution of primes he conjectured that $\pi(n)$ approaches $\dfrac{n}{\log(n) - 1.08366}$ as n increases, a result which is very close to being correct.

Remember that $\pi(n)$ is the number of primes not exceeding n.

In his *Essai* Legendre included an account, together with an attempted proof, of the Law of Quadratic Reciprocity, a result which is to be at the heart of this unit. The relationship given in the Law was first conjectured by Euler in 1783, on the basis of considerable numerical evidence. Two years later Legendre offered the first proof. This proof, like the later one published in *Essai*, contained flaws. In 1795 Gauss, then 18 years old, discovered the Law for himself and in 1798, after what he admitted was a year of strenuous effort, he gave the first correct proof. Gauss acknowledged that, before him, Euler had almost discovered the result and that Legendre knew it and had proved it in various special cases, but he attributed the Law to himself. This brought Legendre and Gauss into conflict. Gauss stuck to his guns that credit for the proof must be given to him on the grounds that all previous proofs were incomplete. Legendre retorted, with good reason, that it was he who had first demonstrated, in detail, how the proof would be achieved. However the gap in Legendre's line of reasoning has not been filled to this day.

In the preceding work we have many times made the statement 'a is a quadratic (non-)residue of p'. There is a convenient shorthand notation for such statements. It was first introduced by Legendre in the course of an incomplete proof of the Law of Quadratic Reciprocity. Naturally enough the notation is named after him.

Definition 2.1 Legendre symbol

Let p be an odd prime and $a \not\equiv 0 \pmod p$. The *Legendre symbol* (a/p) is defined as follows:

$$(a/p) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p, \\ -1, & \text{if } a \text{ is a quadratic non-residue of } p. \end{cases}$$

In other texts the notations $\left(\dfrac{a}{p}\right)$ and $(a|p)$ are sometimes used for the Legendre symbol. Remember that (a/p) does not mean, in any sense, 'a divided by p'.

We read (a/p) as 'a slash p'.

As an illustration of the Legendre symbol we can summarize the results of Example 1.3, which determined the quadratic residues and quadratic non-residues of 13, by writing

$$(1/13) = (3/13) = (4/13) = (9/13) = (10/13) = (12/13) = 1;$$
$$(2/13) = (5/13) = (6/13) = (7/13) = (8/13) = (11/13) = -1.$$

The following theorem contains no essentially new information; it simply collates facts discovered in the previous section about quadratic residues and re-expresses them in terms of the Legendre symbol.

Theorem 2.1 Properties of the Legendre symbol

Let p be an odd prime and let $a \not\equiv 0 \pmod p$ and $b \not\equiv 0 \pmod p$. Then the following properties hold.

(a) If $a \equiv b \pmod p$ then $(a/p) = (b/p)$.

(b) $(a^2/p) = 1$

(c) $(ab/p) = (a/p)(b/p)$

(d) $(a/p) \equiv a^{(p-1)/2} \pmod p$

(e) $(-1/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$

Property (a) says that congruent integers have the same quadratic character. Property (b) makes the obvious claim that any square is a quadratic residue. Property (c) expresses, in succinct form, the multiplicative property of Table 1.1. Property (d) is, of course, Euler's Criterion, and when applied to the particular case $a = -1$ gives the result of property (e), which we have included because we shall refer frequently to this important property.

Problem 2.1

At each stage of the following evaluation of (30/11) state which of the properties of Theorem 2.1 is being used.

$$\begin{aligned}(30/11) &= (8/11), \quad \text{by ?}\\ &= (2/11)(4/11), \quad \text{by ?}\\ &= (2/11), \quad \text{by ?}\\ &= (-9/11), \quad \text{by ?}\\ &= (-1/11)(9/11), \quad \text{by ?}\\ &= (-1/11), \quad \text{by ?}\\ &= -1, \quad \text{by ?}\end{aligned}$$

Diversion

$7 \times 7 = 49$

$67 \times 67 = 4489$

$667 \times 667 = 444889$

$6667 \times 6667 = 44448889$

$66667 \times 66667 = 4444488889$

$666667 \times 666667 = 444444888889$

2.2 Applications using the Legendre symbol

We are going to encounter numerous problems involving quadratic residues. Rather than falling back on first principles, we shall solve them through manipulation of the properties in Theorem 2.1. We begin with two examples illustrating how the Legendre symbol can be used.

Example 2.1

Does the congruence $x^2 + 6x + 11 \equiv 0 \pmod{29}$ have a solution?

As the discriminant is $6^2 - 4 \times 11 = -8$, we must decide whether or not -8 is a quadratic residue of 29, and so we evaluate the Legendre symbol $(-8/29)$.

The properties referred to are those of Theorem 2.1, and throughout congruence is to modulus 29.

$$\begin{aligned}(-8/29) &= (-2/29)(4/29), \quad \text{by property (c),}\\ &= (-2/29), \quad \text{since } (4/29) = 1, \text{ by property (b),}\\ &= (-1/29)(2/29), \quad \text{by property (c),}\\ &= (2/29), \quad \text{since } (-1/29) = 1, \text{ by property (e),}\\ &\equiv 2^{(29-1)/2} = 2^{14}, \quad \text{by property (d),}\\ &\equiv 2^5 \times 2^5 \times 2^4 \equiv 3 \times 3 \times 16\\ &\equiv -1 \pmod{29}.\end{aligned}$$

As the discriminant is a quadratic non-residue we conclude that the congruence does not have a solution. ◆

Example 2.2

Find all the quadratic residues of 37.

We know that 37 has 18 quadratic residues and we could go about finding them by determining the least positive residue modulo 37 of each of 1^2, 2^2, 3^2, …, 18^2, as we did for the prime 11 in Example 1.2. Instead we shall look for some short-cuts.

For a start, we know from property (b) that 1, 4, 9, 16, 25 and 36 are quadratic residues. As $36 \equiv -1 \pmod{37}$, property (a) gives $(-1/37) = 1$, a fact which we could have established alternatively from property (e). Using this together with first property (c) and then property (a):

$$1 = (-1/37)(4/37) = (-4/37) = (33/37),$$

showing that 33 is a quadratic residue. In just the same way, $-9 \equiv 28$, $-16 \equiv 21$ and $-25 \equiv 12$ are quadratic residues of 37.

Having found that 12 and 28 are quadratic residues we can 'remove the square 4' from each, using first property (c) and then property (b):

$$1 = (12/37) = (3/37)(4/37) = (3/37)$$

and

$$1 = (28/37) = (7/37)(4/37) = (7/37).$$

So 3 and 7 are quadratic residues and, again using $(-1/37) = 1$, we find that $-3 \equiv 34$ and $-7 \equiv 30$ are also quadratic residues.

We have now found a total of 14 quadratic residues so there are 4 still to be found. There are many ways of discovering them. For example, reversing the previous procedure and 'multiplying by the square 4' before using property (a):

$$1 = (4/37)(12/37) = (48/37) = (11/37)$$

and

$$1 = (4/37)(16/37) = (64/37) = (27/37),$$

which shows that 11 and 27, and with them their negatives, $-11 \equiv 26$ and $-27 \equiv 10$, are quadratic residues.

The list of quadratic residues of 37 is now complete:

$$1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34 \text{ and } 36.$$ ♦

Problem 2.2

Using only the properties of Theorem 2.1, evaluate the following Legendre symbols.

(a) (3/11) (b) (2/17) (c) (40/11)

Problem 2.3

Show that $(a/31) = 1$ if, and only if, $(2a/31) = 1$. Use this fact to obtain all quadratic residues of 31.

3 GAUSS' LEMMA

3.1 Proof of Gauss' Lemma

One of our objectives in this unit is to prove, and use, the classical theorem known as the Law of Quadratic Reciprocity. This result will be seen to enable us to overcome the computational difficulties of determining the quadratic character of an integer, even for a large integer and large prime modulus. The fascination that this result has had for mathematicians over the years is exemplified by the fact that over 100 proofs of the Law have been published, (seven of them due to Gauss himself — he was not finding further proofs for their own sake but rather trying a find a method of proof which would generalize from the quadratic case to higher powers). The majority of the published proofs hinge on a subsidiary result, Gauss' Lemma, which is the subject matter of this section. Gauss' Lemma offers yet another method of determining the quadratic character of an integer modulo an odd prime and, like Euler's Criterion, while not proving to be a very practicable test when large integers are involved, it is a useful theoretical result for which further applications arise.

Theorem 3.1 Gauss' Lemma

Let p be an odd prime and $a \not\equiv 0 \pmod{p}$. Let S be the set

$$S = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

consisting of the first $\frac{p-1}{2}$ positive multiples of a. If n denotes the number of members of S whose least positive residue modulo p exceeds $\frac{p}{2}$, then $(a/p) = (-1)^n$.

Before setting about the proof we shall look at an example which should serve to clarify the statement of Gauss' Lemma and, more importantly, will illustrate the line to be adopted in the general proof.

Let $p = 19$ and $a = 11$. The set S in Gauss' Lemma consists of the first $\frac{19-1}{2} = 9$ positive multiples of 11:

$$S = \{11, 22, 33, 44, 55, 66, 77, 88, 99\}.$$

Replacing each member of S by its remainder when it is divided by 19, that is, by the least positive residue to which it is congruent modulo 19, we get

$$S' = \{11, 3, 14, 6, 17, 9, 1, 12, 4\}.$$

There are four members, namely 11, 12, 14 and 17, which exceed $\frac{19}{2}$. Hence, according to Gauss' Lemma,

$$(11/19) = (-1)^4 = 1,$$

and we can conclude that 11 is a quadratic residue of 19.

Suppose now that we replace the four members of S' which exceed $\frac{19}{2}$ by their negatives; that is, replace

$$11 \text{ by } -11 \equiv 8, \quad 12 \text{ by } -12 \equiv 7, \quad 14 \text{ by } -14 \equiv 5 \quad \text{and}$$
$$17 \text{ by } -17 \equiv 2 \pmod{19}.$$

This results in the new set

$$S'' = \{8, 3, 5, 6, 2, 9, 1, 7, 4\}.$$

Notice that S'' consists of the first nine positive integers. This is typical of the general situation. The crux of the proof of Gauss' Lemma lies in showing that, for any odd prime p and relatively prime integer a, the set S'', constructed from multiples of a in this way, consists of the first $\dfrac{p-1}{2}$ positive integers. It is a short step from there to completion of the proof.

Returning to our specific example, notice that the product of the elements in S'' is $9!$ while the product of the elements in S is $11^9 \times 9!$. Now the corresponding elements of the sets S and S'' are congruent modulo 19, with the exception of the four sign changes involved in getting from S' to S''. It follows that

$$11^9 \times 9! \equiv (-1)^4 \times 9! \pmod{19}$$

and so, cancelling the $9!$, which is permissible since $\gcd(9!, 19) = 1$,

$$11^9 \equiv 1 \pmod{19}\,.$$

Euler's Criterion now confirms that 11 is indeed a quadratic residue of 19.

The key to the calculation is the number of sign changes in getting from S' to S''. Had this turned out to be an odd integer then we would have had a minus sign remaining in the final congruence and, using Euler's Criterion, we would have concluded that the integer was a quadratic non-residue.

Our proof of Gauss' Lemma retraces the steps of this example working, generally, with any odd prime p and relatively prime integer a.

Proof of Gauss' Lemma

We are given that p is an odd prime, $a \not\equiv 0 \pmod{p}$ and

$$S = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}.$$

First we observe that no two elements of S are congruent modulo p because, if $ra \equiv sa \pmod{p}$ for some integers r and s in the range $1 \leq r, s \leq \dfrac{p-1}{2}$, cancellation would give $r \equiv s \pmod{p}$, which can only happen if $r = s$. Moreover no element of S is congruent modulo p to 0, because $ra \equiv 0 \pmod{p}$, where $a \not\equiv 0 \pmod{p}$ requires $r \equiv 0 \pmod{p}$, which cannot occur.

Let S' be the set obtained by replacing each member of S by its least positive residue modulo p. Putting the elements of S' into increasing order we can write

$$S' = \{b_1, b_2, \ldots, b_m, c_1, c_2, \ldots, c_n\},$$

where $b_m < \dfrac{p}{2} < c_1$ and $m + n = \dfrac{p-1}{2}$. Now let

$$S'' = \{b_1, b_2, \ldots, b_m, p - c_1, p - c_2, \ldots, p - c_n\}.$$

Note that $\dfrac{p}{2}$ is not an integer so neither b_m nor c_1 can be equal to $\dfrac{p}{2}$.

It is our contention that $S'' = \left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$. Certainly the integers listed in S'' are all positive, there are $\dfrac{p-1}{2}$ of them, and the largest is either b_m or $p - c_1$, each of which is less than $\dfrac{p}{2}$. Hence there are $\dfrac{p-1}{2}$ positive integers each less than $\dfrac{p}{2}$, and so to justify our contention we need only show that they are distinct.

Note that this does not imply that $b_1 = 1$, $b_2 = 2$, etc. as the elements may be written in a different order.

As the elements of S' are distinct, the m elements b_1, b_2, …, b_m are distinct, as are the n elements $p - c_1$, $p - c_2$, …, $p - c_n$. So suppose that $b_i = p - c_j$, for some i and j. Then,

$$p = b_i + c_j \equiv ra + sa \pmod{p}\,,$$

for some integers r and s in the range $1 \le r, s \le \frac{p-1}{2}$. But from

$$p \equiv (r+s)a \pmod{p} \text{ and } a \not\equiv 0 \pmod{p},$$

Euclid's Lemma leads to $r + s \equiv 0 \pmod{p}$, which is impossible since $2 \le r + s \le p - 1$.

This establishes that

$$S'' = \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}.$$

We continue by multiplying the elements of S'' together:

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= b_1 b_2 \ldots b_m (p - c_1)(p - c_2)\ldots(p - c_n)\\ &\equiv b_1 b_2 \ldots b_m (-c_1)(-c_2)\ldots(-c_n) \pmod{p}\\ &\equiv (-1)^n b_1 b_2 \ldots b_m c_1 c_2 \ldots c_n \pmod{p}\\ &\equiv (-1)^n a \times 2a \times 3a \times \ldots \times \frac{p-1}{2} a \pmod{p}\\ &\equiv (-1)^n \times a^{(p-1)/2} \times \left(\frac{p-1}{2}\right)! \pmod{p}.\end{aligned}$$

This step following from the fact that the elements of S' are congruent, in some order, to the elements of S.

Now $\gcd\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$ and so the term $\left(\frac{p-1}{2}\right)!$ may be cancelled from the two sides of the congruence leaving

$$1 \equiv (-1)^n a^{(p-1)/2} \pmod{p}.$$

Finally we appeal to Euler's Criterion in the form of property (d) of Theorem 2.1, that $a^{(p-1)/2} \equiv (a/p) \pmod{p}$, and then multiply both sides of the congruence by $(-1)^n$ to obtain

$$(a/p) = (-1)^n. \qquad \blacksquare$$

Gauss' Lemma can be used in a very straightforward way to determine Legendre symbols: just write down the set S, convert it to the set S' and count how many members of S' lie in the appropriate range. Providing the prime modulus is not large the arithmetic involved in doing this is not taxing.

Problem 3.1

Use Gauss' Lemma to evaluate the following Legendre symbols.

(a) $(7/13)$ (b) $(11/23)$ (c) $(5/29)$

3.2 Applications of Gauss' Lemma

In order to evaluate (n/p) for any positive integer $n > 1$ and odd prime p which does not divide n, consider the prime decomposition

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}.$$

Property (b) of Theorem 2.1 establishes that $(1/p) = 1$, so we need not consider $n = 1$ further.

Repeated application of the multiplicative property of the Legendre symbol, Theorem 2.1, property (c), leads to

$$(n/p) = (p_1/p)^{k_1}(p_2/p)^{k_2}\ldots(p_r/p)^{k_r}.$$

Now in considering Legendre symbols we must not overlook negative integers. Note that

$$-n = (-1)p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$$

and using the multiplicative property again we have

$$(-n/p) = (-1/p)(p_1/p)^{k_1}(p_2/p)^{k_2}\dots(p_r/p)^{k_r}.$$

So, to evaluate (a/p) for any integer a not divisible by the odd prime p, it suffices to be able to calculate $(-1/p)$, $(2/p)$ and (p_i/p) for any odd prime $p_i \neq p$. We have already dealt with $(-1/p)$ in property (e) of Theorem 2.1. Evaluation of the general (p_i/p) will be postponed until we have the Law of Quadratic Reciprocity at our disposal. However, Gauss' Lemma will resolve the $(2/p)$ problem for us.

As $-1 \equiv p-1 \pmod p$ we can do without $(-1/p)$, however, using it is often a more efficient way to proceed.

Theorem 3.2 The quadratic character of 2

If p is an odd prime then

$$(2/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8, \\ -1, & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8. \end{cases}$$

The result can be expressed in either of the alternative forms

$$(2/p) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8, \\ -1, & \text{if } p \equiv \pm 3 \pmod 8, \end{cases}$$

or $(2/p) = (-1)^{(p^2-1)/8}$.

Proof of Theorem 3.2

To bring Gauss' Lemma to bear we observe that $(2/p) = (-1)^n$, where n is the number of integers in the set

$$S = \left\{2\times 1,\ 2\times 2,\ 2\times 3,\ \dots,\ 2\times\frac{p-1}{2}\right\}$$
$$= \{2, 4, 6, \dots, p-1\}$$

which have least positive residue modulo p exceeding $\frac{p}{2}$. The integers in S are, as they stand, least positive residues of p and so our task is to count how many of them exceed $\frac{p}{2}$.

Now $2k > \frac{p}{2}$ if, and only if, $k > \frac{p}{4}$. It follows that the first $\operatorname{int}\left(\frac{p}{4}\right)$ multiples of 2 do not exceed $\frac{p}{2}$, where $\operatorname{int}(x)$ denotes the integer part of x; that is, the largest integer which does not exceed x.

The remaining multiples do exceed $\frac{p}{2}$. So

$$n = \frac{p-1}{2} - \operatorname{int}\left(\frac{p}{4}\right).$$

There are four cases to consider corresponding to the four possible congruence classes modulo 8 of the odd prime p:

(i) $p = 8k+1 \Longrightarrow n = 4k - \operatorname{int}\left(2k+\frac{1}{4}\right) = 4k - 2k = 2k$;

(ii) $p = 8k+3 \Longrightarrow n = 4k+1 - \operatorname{int}\left(2k+\frac{3}{4}\right) = 4k+1-2k = 2k+1$;

(iii) $p = 8k+5 \Longrightarrow n = 4k+2 - \operatorname{int}\left(2k+\frac{5}{4}\right) = 4k+2-(2k+1) = 2k+1$;

(iv) $p = 8k+7 \Longrightarrow n = 4k+3 - \operatorname{int}\left(2k+\frac{7}{4}\right) = 4k+3-(2k+1) = 2k+2$.

In cases (i) and (iv), n is even and so $(2/p) = 1$. In cases (ii) and (iii), n is odd and so $(2/p) = -1$. ■

Problem 3.2

Write down the values of the following Legendre symbols.

(a) (2/29) (b) (2/31) (c) (2/43)

Problem 3.3

Adapt the proof of Theorem 3.2 to show that

$$(-2/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 3 \pmod 8, \\ -1, & \text{if } p \equiv 5 \pmod 8 \text{ or } p \equiv 7 \pmod 8. \end{cases}$$

Problem 3.4

Check the result of Problem 3.3 by confirming that

$$(-2/p) = (-1/p)(2/p)$$

holds.

The result of Theorem 3.2 provides us with a neat proof of Theorem 2.2 of *Unit 5*. The result in question concerned the Mersenne numbers $M_n = 2^n - 1$.

Theorem 3.3 (Theorem 2.2 of Unit 5)

If p and $2p+1$ are both primes, where $p \equiv 3 \pmod 4$ then $2p+1$ divides M_p.

This result was stated without proof in *Unit 5*.

Proof of Theorem 3.3

Let q be the prime $2p+1$. From $p = 4k+3$ we have $2p+1 = 8k+7$ and so $q \equiv 7 \pmod 8$. Now Theorem 3.2 gives $(2/q) = 1$, so that 2 is a quadratic residue of q. Euler's Criterion gives $2^{(q-1)/2} \equiv (2/q) \pmod q$, and putting the two together gives $2^{(q-1)/2} \equiv 1 \pmod q$. That is, q divides $2^{(q-1)/2} - 1$ which, when q is replaced by $2p+1$, says that $2p+1$ divides M_p, as claimed. ■

As we saw in *Unit 5* this result shows that M_{11}, M_{23}, M_{83} and numerous other Mersenne numbers are composite. It remains an unsolved problem whether the list we have begun here extends infinitely; that is, it is not known whether there are infinitely many primes p of the form $4k+3$ for which $2p+1$ is also prime.

3.3 More cases of Dirichlet's Theorem

In *Unit 2* we mentioned, without proof, Dirichlet's Theorem which asserts that, for relatively prime positive integers a and b, there are infinitely many primes of the form $ak+b$. We proved some special instances of this result including the infinitude of primes of the form $4k+3$. In a curious way our results on quadratic residues will lead to proofs of many more particular instances of Dirichlet's result. As *Unit 2* posed the question of whether or not there are infinitely many primes of the form $4k+1$, this is the obvious starting point for us here.

Theorem 3.4

There are infinitely many primes of the form $4k+1$.

Proof of Theorem 3.4

Aiming for a contradiction, suppose that there are only a finite number of primes of the form $4k+1$, say $p_1, p_2, \ldots, p_n$.

Let $N = (2p_1p_2\ldots p_n)^2 + 1$. As N is odd it must be divisible by some odd prime, say p. Then $(2p_1p_2\ldots p_n)^2 \equiv -1 \pmod{p}$. As the term on the left of this congruence is a square we can infer that $(-1/p) = 1$ and then, by virtue of property (e) of Theorem 2.1, that p is of the form $4k+1$. The assumption that $p_1, p_2, \ldots, p_n$ are the only primes of this form forces $p = p_i$, for some i. But this means that p divides $(2p_1p_2\ldots p_n)^2$, and coupling this fact with p divides N we conclude that p divides $N - (2p_1p_2\ldots p_n)^2$. That is, p divides 1, and we have the required contradiction.

Hence there are infinitely many primes of the form $4k+1$. ■

Although we presented the proof of Theorem 3.4 as one by contradiction the essence of the argument was to show that from any list of primes of the form $4k+1$ we can always discover another prime of the same form. From the list $p_1, p_2, \ldots, p_n$ we constructed $(2p_1p_2\ldots p_n)^2 + 1$ which has to be divisible by a prime of form $4k+1$ which is not one of the original list. Many special instances of Dirichlet's result can be proved in more or less this way, the key to the proof being in finding the 'new' number to construct. In our next example we use a similar method but with an extra step like the one used previously in our corresponding proof that there are infinitely many primes of the form $4k+3$.

Theorem 3.5

There are infinitely many primes of the form $8k-1$.

Integers of the form $8k-1$ are equally well expressed as integers of the form $8k+7$

Proof of Theorem 3.5

Suppose that there are only finitely many primes of the form $8k-1$. If there are only finitely many then there is a largest such prime, say P. Consider the integer $N = 2(P!)^2 - 1$. As $P!$ is even, $2(P!)^2$ is divisible by 8 and so $N \equiv -1 \pmod{8}$.

Being odd, N has an odd prime divisor. Let p be such a divisor. Then $2(P!)^2 \equiv 1 \pmod{p}$. So

$$(2/p)((P!)^2/p) = (1/p),$$

and as $(P!)^2$ and 1 are both squares we deduce that $(2/p) = 1$. Bringing Theorem 3.2 into play, p is congruent modulo 8 to either 1 or -1. Now any product of integers congruent modulo 8 to 1 is itself congruent modulo 8 to 1. As N is not of this form, at least one of its prime divisors, say q, must be congruent modulo 8 to -1. The assumption that the largest prime of this form is P tells us that $q \leq P$. But then q divides $2(P!)^2$ and as q divides $2(P!)^2 - 1$, we must have q divides 1, a contradiction.

Hence there are infinitely many primes of the form $8k-1$. ■

Problem 3.5

Show that there are infinitely many primes of the form $8k+3$ by the following method. Suppose that there are only a finite number of primes of form $8k+3$, namely $p_1, p_2, \ldots, p_n$. Consider the integer $N = (p_1p_2\ldots p_n)^2 + 2$. For any prime divisor p of N show that $(-2/p) = 1$ and deduce that N must have a prime divisor of the form $8k+3$. Reach a contradiction by noting that this prime would have to be one of the original list $p_1, p_2, \ldots, p_n$.

4 THE LAW OF QUADRATIC RECIPROCITY

4.1 Understanding the law

This section is concerned with the Law of Quadratic Reciprocity which, for ease of reference, we shall abbreviate to LQR. Amongst its numerous applications, LQR provides us with a new method for simplifying Legendre symbols. However, unlike the preceding methods, LQR is simple to employ even when the integers in question are large.

Before we confront the difficult task of proving LQR we shall begin by illustrating the implications of the result through some simple examples.

Theorem 4.1 The Law of Quadratic Reciprocity

If p and q are distinct odd primes then

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}.$$

This bland statement probably does not mean much to you yet. Let us hold fire for a moment and express the statement of LQR in a slightly different way to clarify just what it entails. Look at the expression $(-1)^{(p-1)(q-1)/4}$ and suppose that $p \equiv 1 \pmod 4$. In this case $p-1$ is divisible by 4 and, since $q-1$ is also even, $\dfrac{(p-1)(q-1)}{4}$ is an even integer. Therefore $(-1)^{(p-1)(q-1)/4} = 1$. Similarly if $q \equiv 1 \pmod 4$ then $(-1)^{(p-1)(q-1)/4} = 1$. On the other hand, if $p \equiv q \equiv 3 \pmod 4$ then $p-1$ and $q-1$ are each equal to twice an odd integer and so $\dfrac{(p-1)(q-1)}{4}$ is odd. In this case $(-1)^{(p-1)(q-1)/4} = -1$. The statement of LQR can now be given in the alternative form:

$$(p/q)(q/p) = \begin{cases} 1, & \text{if either } p \equiv 1 \pmod 4 \quad \text{or} \quad q \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

But we can take this a step further. As (p/q) and (q/p) are each equal to either 1 or -1, their product $(p/q)(q/p)$ will be equal to 1 precisely when $(p/q) = (q/p)$ and will be equal to -1 precisely when $(p/q) = -(q/p)$. We therefore have the following way of stating LQR which will prove to be a more useful way of looking at it in many practical situations.

Theorem 4.2 An alternative formulation of LQR

If p and q are distinct odd primes then

$$(p/q) = \begin{cases} (q/p), & \text{if either } p \equiv 1 \pmod 4 \quad \text{or} \quad q \equiv 1 \pmod 4, \\ -(q/p), & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

LQR provides the missing link in the processes required to evaluate any Legendre symbol (a/p), where a is an integer not divisible by the odd prime p. We have seen that it is sufficient to be able to evaluate $(-1/p), (2/p)$ and (q/p), for any odd prime $q \neq p$. We have found simple formulae for $(-1/p)$ and $(2/p)$. LQR now provides the means of determining (q/p). We shall illustrate the method by an example.

Example 4.1

Is 31 a quadratic residue of 73?

We need to evaluate the Legendre symbol (31/73).

$$\begin{aligned}
(31/73) &= (73/31), && \text{by LQR, noting that } 73 \equiv 1 \pmod 4,\\
&= (11/31), && \text{since } 73 \equiv 11 \pmod{31},\\
&= (-1)(31/11), && \text{by LQR, noting that } 11 \equiv 31 \equiv 3 \pmod 4,\\
&= (-1)(9/11), && \text{since } 31 \equiv 9 \pmod{11},\\
&= -1, && \text{since 9 is a square.}
\end{aligned}$$

So 31 is not a quadratic residue of 73. ◆

The underlying process illustrated in this example is that the evaluation of any Legendre symbol is achieved by replacing it by a product of one or more simpler Legendre symbols, simpler in the sense that the integers involved in the symbol are smaller. LQR is needed to simplify the Legendre symbol (p/q), where $p < q$, by replacing it with either (q/p) or $(-1)(q/p)$, whichever is the case. As $p < q$, the symbol (q/p) can then be simplified by, for example, replacing q by its least positive residue modulo p (which is allowed by property (a) of Theorem 2.1). As the integers are repeatedly reduced, a stage will be reached when the value of the Legendre symbol is known.

The next example is similar, but involves a larger prime, 229. We have illustrated the breakdown into 'smaller' Legendre symbols schematically.

Example 4.2

Determine the Legendre symbol (−134/229).

$$\begin{tikzcd}
 & & (-134/229) \arrow[d, "2.1(c)"] & & & \\
(-1/229) \arrow[d, "2.1(e)"] & \times & (2/229) \arrow[d, "3.2"] & \times & (67/229) \arrow[d, "\text{LQR}"] & \\
1 & \times & (-1) & \times & (229/67) \arrow[d, "2.1(a)"] & \\
 & & & & (28/67) \arrow[d, "2.1(c)"] & \\
 & & & (4/67) \arrow[d, "2.1(b)"] & \times & (7/67) \arrow[d, "\text{LQR}"] \\
 & & & 1 & \times & (-1) \times (67/7) \arrow[d, "2.1(a)"] \\
 & & & & & (4/7) \arrow[d, "2.1(b)"] \\
 & & & & & 1
\end{tikzcd}$$

So $(-134/229) = 1 \times (-1) \times 1 \times (-1) \times 1 = 1$. ◆

Problem 4.1

Determine the following Legendre symbols.

(a) (−219/383) (b) (461/773)

The integers 383, 461 and 773 are primes.

Problem 4.2

Explain each of the steps in the following evaluation of the Legendre symbol (164/197).

$$\begin{aligned}(164/197) &= (4/197)(41/197)\\ &= (41/197)\\ &= (197/41)\\ &= (74/41)\\ &= (2/41)(37/41)\\ &= (37/41)\\ &= (41/37)\\ &= (4/37)\\ &= 1.\end{aligned}$$

Problem 4.3

The following evaluation of (60/79) contains a number of errors involving misuse of LQR and properties of the Legendre symbol. Identify the errors.

$$\begin{aligned}(60/79) &= (-19/79), \quad \text{since } 60 \equiv -19 \pmod{79},\\ &= (-1)(19/79), \quad \text{since } -19 = (-1)\times 19,\\ &= (-1)(79/19), \quad \text{by LQR},\\ &= (-1)(60/19), \quad \text{since } 79 \equiv 60 \pmod{19},\\ &= (-1)(4/19)(15/19), \quad \text{since } 60 = 4\times 15,\\ &= (-1)(15/19), \quad \text{since 4 is a square},\\ &= (-1)(-1)(19/15), \quad \text{by LQR, noting that } 15 \equiv 19 \equiv 3 \pmod 4,\\ &= (4/15), \quad \text{since } 19 \equiv 4 \pmod{15},\\ &= 1, \quad \text{since 4 is a square.}\end{aligned}$$

4.2 Proof of LQR

Since the first proof, given by Gauss, over 100 further proofs have been published. None of them is short and snappy! The one that we have opted to give here was discovered by one of Gauss' students, Ferdinand Eisenstein and, like many of the published proofs, builds on Gauss' Lemma. The proof is really in two distinct parts, the first of which establishes the link between LQR and Gauss' Lemma. To make the proof easier to understand we shall establish the first part as a separate result.

Theorem 4.3

Let p be an odd prime and a an odd integer not divisible by p. Then

$$(a/p) = (-1)^{\alpha(a,p)},$$

where

$$\alpha(a,p) = \sum_{k=1}^{(p-1)/2} \operatorname{int}\left(\frac{ka}{p}\right).$$

To clarify the statement of the theorem take the case $a = 5$ and $p = 13$. Then $\alpha(5,13)$ comprises the sum of $\dfrac{13-1}{2} = 6$ terms:

$$\begin{aligned}\alpha(5,13) &= \operatorname{int}\left(\frac{5}{13}\right) + \operatorname{int}\left(\frac{10}{13}\right) + \operatorname{int}\left(\frac{15}{13}\right) + \operatorname{int}\left(\frac{20}{13}\right) + \operatorname{int}\left(\frac{25}{13}\right) + \operatorname{int}\left(\frac{30}{13}\right)\\ &= 0+0+1+1+1+2 = 5,\end{aligned}$$

and so, according to the theorem, $(5/13) = (-1)^5 = -1$.

Proof of Theorem 4.3

Exactly as in our proof of Gauss' Lemma, we consider the set of integers

$$S = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

and, replacing each integer by its least positive residue modulo p and listing the integers in ascending order, we reach

$$S' = \{b_1, b_2, \ldots, b_m, c_1, c_2, \ldots, c_n\},$$

where $b_m < \frac{p}{2} < c_1$. Now, according to the Division Algorithm, if we divide any $ka \in S$ by p we get

$$ka = p \times \operatorname{int}\left(\frac{ka}{p}\right) + \text{remainder},$$

where the remainder is one of the integers in S'. Allowing k to run from 1 to $\frac{p-1}{2}$ and adding up the resulting equations we get

As in the proof of Gauss' Lemma, the remainders which occur are distinct members of S'.

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} p \times \operatorname{int}\left(\frac{ka}{p}\right) + \sum_{i=1}^{m} b_i + \sum_{j=1}^{n} c_j. \qquad (*)$$

In the proof of Gauss' Lemma we went on to show that the set

$$\begin{aligned} S'' &= \{b_1, b_2, \ldots, b_m, p - c_1, p - c_2, \ldots, p - c_n\} \\ &= \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}. \end{aligned}$$

Adding the integers in this set gives

$$\sum_{k=1}^{(p-1)/2} k = \sum_{i=1}^{m} b_i + \sum_{j=1}^{n} (p - c_j) = \sum_{i=1}^{m} b_i + pn - \sum_{j=1}^{n} c_j.$$

Subtracting this equation from $(*)$ gives

$$\sum_{k=1}^{(p-1)/2} ka - \sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{(p-1)/2} p \times \operatorname{int}\left(\frac{ka}{p}\right) + 2 \times \sum_{j=1}^{n} c_j - pn.$$

That is,

$$(a-1) \sum_{k=1}^{(p-1)/2} k = p \times \alpha(a,p) + 2 \times \sum_{j=1}^{n} c_j - pn.$$

Finally we write this equation modulo 2, noting that each of the terms still involving summation is even (since a is odd):

$$p\alpha(a,p) - pn \equiv 0 \pmod{2}.$$

Since p is odd this amounts to $\alpha(a,p) \equiv n \pmod{2}$. From the conclusion of Gauss' Lemma that $(a/p) = (-1)^n$ we have reached $(a/p) = (-1)^{\alpha(a,p)}$, as claimed. ■

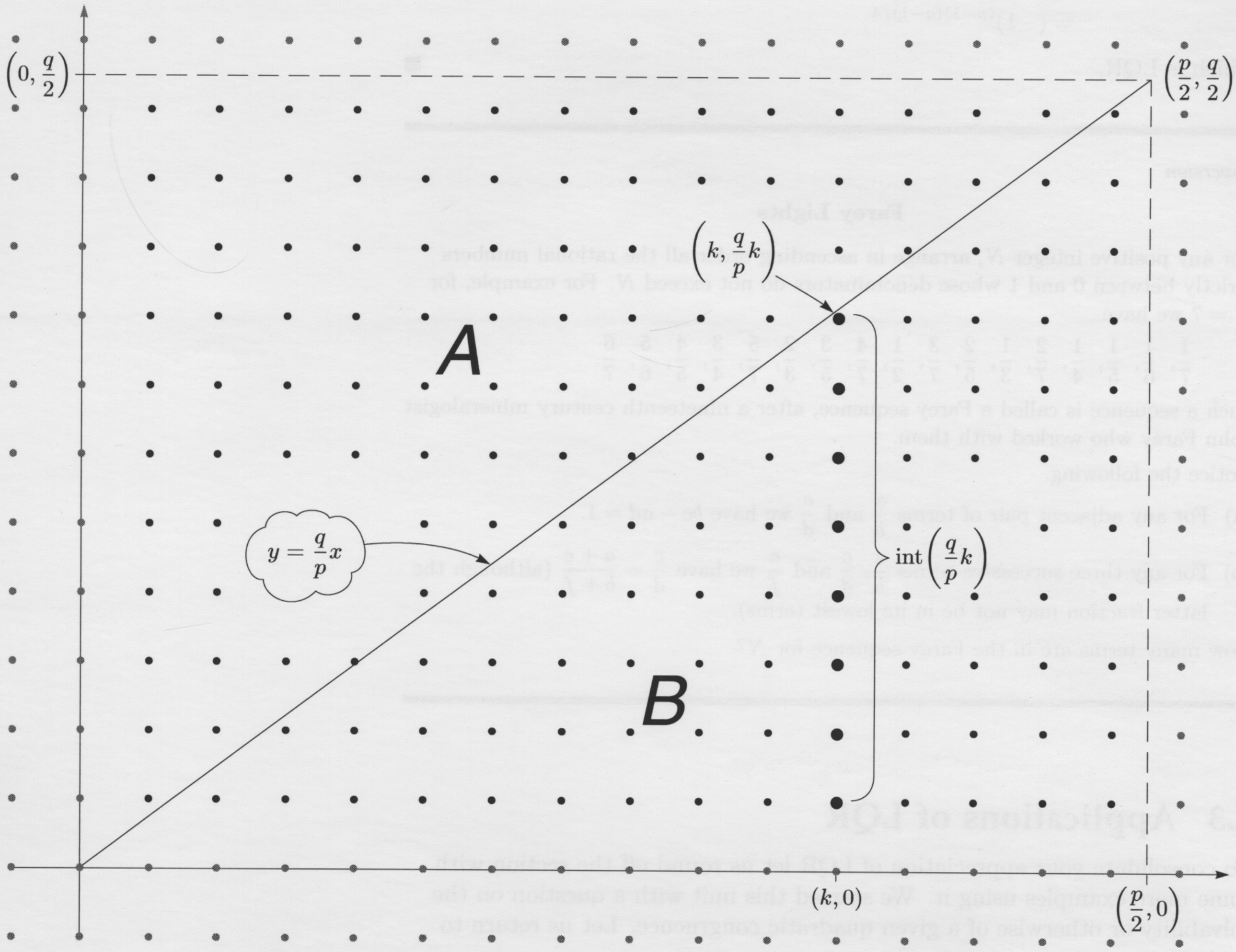
With this result at our disposal it is just a short step to completion of the proof of LQR.

Proof of LQR

For the given odd primes p and q, consider the rectangle in the xy-plane which has vertices at (0,0), $\left(\frac{p}{2}, 0\right)$, $\left(\frac{p}{2}, \frac{q}{2}\right)$ and $\left(0, \frac{q}{2}\right)$. The number of lattice points *inside* this rectangle is $\frac{p-1}{2} \times \frac{q-1}{2}$. Consider the diagonal from (0,0) to $\left(\frac{p}{2}, \frac{q}{2}\right)$, which has equation $y = \frac{q}{p}x$. Inside the rectangle there

Lattice points are points (a, b), where each of a and b is an integer.

are no lattice points on this diagonal, because if (a, b) is a lattice point on this diagonal then $b = \frac{q}{p}a$. But as p and q are distinct primes, this implies that p divides a and q divides b, which forces (a, b) outside the rectangle.



$\left(0, \frac{q}{2}\right)$
$\left(\frac{p}{2}, \frac{q}{2}\right)$
$\left(k, \frac{q}{p}k\right)$
A
$y = \frac{q}{p}x$
$\text{int}\left(\frac{q}{p}k\right)$
B
$(k, 0)$
$\left(\frac{p}{2}, 0\right)$

Figure 4.1

Denote by A and B the triangular regions inside the rectangle which lie respectively above and below the diagonal. For integer k with $0 < k < \frac{p}{2}$ the number of lattice points in B lying directly above the point $(k, 0)$ on the x-axis is $\text{int}\left(\frac{q}{p}k\right)$. Hence the total number of lattice points in B is

$$\sum_{k=1}^{(p-1)/2} \text{int}\left(\frac{q}{p}k\right),$$

which is $\alpha(q, p)$. In the same way, by counting the lattice points to the right of $(0, k)$, the total number of lattice points in A is $\alpha(p, q)$. Now the number of lattice points in A added to the number of lattice points in B is the total number of lattice points in the rectangle which is

The argument is symmetrical with the roles of p and q interchanged.

$$\frac{p-1}{2} \times \frac{q-1}{2} = \frac{(p-1)(q-1)}{4}.$$

Hence, from the two ways of counting the number of lattice points

$$\alpha(p, q) + \alpha(q, p) = \frac{(p-1)(q-1)}{4}.$$

The equality of the two counts uses the fact that there are no points on the diagonal.

So, in terms of Legendre symbols, by Theorem 4.3,

$$\begin{aligned}(p/q)(q/p) &= (-1)^{\alpha(p,q)} \times (-1)^{\alpha(q,p)} \\ &= (-1)^{\alpha(p,q)+\alpha(q,p)} \\ &= (-1)^{(p-1)(q-1)/4},\end{aligned}$$

which is LQR. ■

Diversion

Farey Lights

For any positive integer N, arrange in ascending order all the rational numbers strictly between 0 and 1 whose denominators do not exceed N. For example, for $N = 7$ we have

$$\frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}.$$

Such a sequence is called a Farey sequence, after a nineteenth century mineralogist John Farey who worked with them.

Notice the following.

(a) For any adjacent pair of terms $\frac{a}{b}$ and $\frac{c}{d}$ we have $bc - ad = 1$.

(b) For any three successive terms $\frac{a}{b}$, $\frac{c}{d}$ and $\frac{e}{f}$ we have $\frac{c}{d} = \frac{a+e}{b+f}$ (although the latter fraction may not be in its lowest terms).

How many terms are in the Farey sequence for N?

4.3 Applications of LQR

To consolidate your appreciation of LQR let us round off the section with some more examples using it. We started this unit with a question on the solvability or otherwise of a given quadratic congruence. Let us return to that theme.

Example 4.3

Does the congruence $3x^2 - 8x - 5 \equiv 0 \pmod{139}$ have any solutions?

139 is prime.

The discriminant of the quadratic is

$$(-8)^2 - 4 \times 3 \times (-5) = 124,$$

so the question boils down to the determination of the Legendre symbol (124/139). In what follows we use, in addition to LQR, the various Legendre symbol properties of Theorem 2.1. In the explanation of the steps we highlight the property being used, rather than refer to which one it is.

$$\begin{aligned}(124/139) &= (4/139)(31/139), \quad \text{using } 124 = 4 \times 31, \\ &= 1 \times (31/139), \quad \text{since } 4 = 2^2, \\ &= (-1)(139/31), \quad \text{by LQR, since } 31 \equiv 139 \equiv 3 \pmod{4}, \\ &= (-1)(15/31), \quad \text{since } 139 \equiv 15 \pmod{31}, \\ &= (-1)(3/31)(5/31), \quad \text{using } 15 = 3 \times 5, \\ &= (-1)(-1)(31/3)(5/31), \quad \text{by LQR, since } 31 \equiv 3 \pmod{4}, \\ &= (31/3)(31/5), \quad \text{by LQR, since } 5 \equiv 1 \pmod{4}, \\ &= (1/3)(31/5), \quad \text{since } 31 \equiv 1 \pmod{3}, \\ &= (1/3)(1/5), \quad \text{since } 31 \equiv 1 \pmod{5}, \\ &= 1.\end{aligned}$$

The congruence does have solutions. ◆

Problem 4.4

For each of the following congruences decide whether or not it has any solutions.

(a) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$

(b) $2x^2 + 5x - 9 \equiv 0 \pmod{11 \times 101}$

Which primes $p \geq 5$ have 3 as a quadratic residue? In terms of the Legendre symbol we are asking: which primes p satisfy $(3/p) = 1$? LQR gives us a start in tackling this one. Since $3 \equiv 3 \pmod 4$, the result of applying LQR to $(3/p)$ depends on the value of p modulo 4:

$$(3/p) = \begin{cases} (p/3), & \text{if } p \equiv 1 \pmod 4, \\ (-1)(p/3), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now the least positive residue of p modulo 3 is either 1 (which is a square) or 2 (which is not), so:

$$(p/3) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 3, \\ -1, & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

The two parts need to be combined to obtain the value of $(3/p)$, and for that we need to consider values of p to both modulus 3 and modulus 4; so we look at cases modulo 12. For example, if $p \equiv 7 \pmod{12}$ then we have $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 3$. Therefore

$$(3/p) = (-1)(p/3) \quad \text{and} \quad (p/3) = 1$$

which combine to give $(3/p) = -1$.

There are, in all, four possible values modulo 12 which a prime (greater than 3) can take, namely $p \equiv 1, 5, 7$ or $11 \pmod{12}$. The value of $(3/p)$ in each case is as determined in the table below.

	$p \pmod 3$	$(p/3)$	$p \pmod 4$	$(3/p)$
$p \equiv 1 \pmod{12}$	1	1	1	1
$p \equiv 5 \pmod{12}$	2	-1	1	-1
$p \equiv 7 \pmod{12}$	1	1	3	-1
$p \equiv 11 \pmod{12}$	2	-1	3	1

We can summarize these findings as follows.

Theorem 4.4 The quadratic character of 3

If $p > 3$ is prime then

$$(3/p) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1, & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Problem 4.5

For which primes $p > 3$ is $(6/p) = 1$?

Problem 4.6

Prove that, for prime $p > 3$, $(-3/p) = 1$ if, and only if, $p \equiv 1 \pmod 6$. Use this to prove that there are infinitely many primes of the form $6k + 1$ by considering the integer $(2p_1p_2 \dots p_n)^2 + 3$, where $p_1, p_2, \dots, p_n$ are assumed to be the only primes of the form $6k + 1$.

We have achieved the main goal of this unit. Given any quadratic congruence with prime modulus we can decide whether or not it has solutions. Moreover part (b) of Problem 4.4 illustrates a fruitful line of approach for similar problems where the modulus is a product of distinct primes. As far as general composite moduli are concerned there is one idea of particular interest in our present situation which merits mention. The Legendre symbol can be generalized in a simple way.

Definition 4.1 The Jacobi symbol

Let m and n be integers, with n odd, $n \geq 3$ and $\gcd(m, n) = 1$. Writing $n = p_1 p_2 \cdots p_r$ as a product of (not necessarily distinct) primes, then the Jacobi symbol (m/n) is defined by

$$(m/n) = (m/p_1)(m/p_2)\ldots(m/p_r),$$

where the symbols on the right-hand side are Legendre symbols.

So, for example,

$$(14/275) = (14/5)(14/5)(14/11) = (4/5)(4/5)(3/11) = 1 \times 1 \times 1 = 1.$$

By Theorem 4.4, $(3/11) = 1$.

From our knowledge of Legendre symbols there is little remaining challenge in evaluating Jacobi symbols. But what does the Jacobi symbol represent? It would be nice if, for odd relatively prime integers m and n we had $(m/n) = 1$ if, and only if, m is a non-zero square modulo n. Unfortunately this is not true. For example, 5 is not a square modulo 9, but

$$(5/9) = (5/3)(5/3) = (2/3)(2/3) = (-1)(-1) = 1.$$

We talk about 'squares' rather than quadratic residues because the latter are defined only for prime modulus.

But all is not lost because it is true that if $(m/n) = -1$ then m is not a square modulo n. To see this, suppose that $(m/n) = -1$. Then in the expression of (m/n) as a product of Legendre symbols there is (at least) one prime divisor p of n for which $(m/p) = -1$. That is, m is not a square modulo p. It follows that m cannot be a square modulo n.

If $x^2 \equiv m \pmod{n}$ then $x^2 \equiv m \pmod{d}$ for any divisor d of n.

The Jacobi symbol (m/n) is a generalization of the Legendre symbol in that the two notions coincide when n is prime. In fact, almost all the properties we have seen for the Legendre symbol do generalize. In particular the following all hold true; we state them without proof.

If m and n are odd integers both exceeding 1 with $\gcd(m, n) = 1$, then:

(a) $(-1/n) = (-1)^{(n-1)/2}$, Euler's Criterion;

(b) $(2/n) = (-1)^{(n^2-1)/8}$, Theorem 3.2;

(c) $(m/n)(n/m) = (-1)^{(m-1)(n-1)/4}$, LQR.

ADDITIONAL EXERCISES

Section 1

1 Solve the following congruences.

(a) $2x^2 + 4x + 1 \equiv 0 \pmod{7}$

(b) $3x^2 + x - 3 \equiv 0 \pmod{11}$

2 For which integers c does the congruence $2x^2 - 5x + c \equiv 0 \pmod{13}$ have solutions? Solve the congruence for the case $c = 1$.

The quadratic residues of 13 are found in Example 1.3.

3 Use Euler's Criterion to determine whether or not 3 is a quadratic residue of the following primes.

(a) 23 (b) 29

4 Quadratic residues can be defined for composite $n > 2$ by analogy with the prime case. Each integer a satisfying $\gcd(a, n) = 1$ is either a quadratic residue or non-residue of n depending on whether or not the congruence $x^2 \equiv a \pmod{n}$ has solutions.

Prove that if a is a quadratic residue of n then $a^{\phi(n)/2} \equiv 1 \pmod{n}$. Show that the converse of this result is false by exhibiting relatively prime integers a and n for which $a^{\phi(n)/2} \equiv 1 \pmod{n}$ but for which $x^2 \equiv a \pmod{n}$ has no solutions.

Remember that $\phi(n)$ is even for $n > 2$ and so $\phi(n)/2$ is an integer.

Section 2

1 Making use of properties of Theorem 2.1, determine whether or not the following congruences have solutions.

(a) $x^2 + 8x + 4 \equiv 0 \pmod{13}$

(b) $x^2 + 7x + 9 \equiv 0 \pmod{23}$

2 Evaluate the following Legendre symbols.

(a) $(18/19)$ (b) $(45/19)$ (c) $(2/19)$

3 Confirm that $(-1/29) = 1$ and hence that ± 1, ± 4, ± 9, and ± 16 are quadratic residues of 29. Determine the remaining quadratic residues of 29.

4 If p is an odd prime and $\gcd(a, p) = 1$ deduce, using Euler's Criterion and Wilson's Theorem, that

$$(p-1)! \equiv -(a/p)a^{(p-1)/2} \pmod{p}.$$

Section 3

1 Use Gauss' Lemma to determine the following Legendre symbols.

(a) $(-3/13)$ (b) $(5/17)$

2 Show that 2 is a quadratic residue of:

(a) every prime of the form $4^n + 1$, for $n > 1$;

(b) every Mersenne prime $M_p = 2^p - 1$, except $M_2 = 3$;

(c) every Fermat prime $F_n = 2^{2^n} + 1$, for $n > 1$.

For each of these primes decide whether or not -2 is a quadratic residue.

3 Show that there are infinitely many primes of the form $8k + 5$ in the following way. Suppose that $p_1, p_2, \ldots, p_n$ are the only primes of this form and reach a contradiction by considering the integer

$$N = 4(p_1 p_2 \ldots p_n)^2 + 1.$$

Section 4

1 Evaluate the following Legendre symbols.

(a) $(35/71)$ (b) $(139/149)$ (c) $(1234/4567)$

The integers 139, 149 and 4567 are all primes.

2 Which of the following congruences have solutions?

(a) $3x^2 + x - 7 \equiv 0 \pmod{17}$

(b) $2x^2 + x + 1 \equiv 0 \pmod{29}$

(c) $2x^2 + 3x - 7 \equiv 0 \pmod{101}$

3 (a) If p and $q = 10p + 3$ are odd primes, show that $(p/q) = (3/p)$.

(b) If p and $q = 10p + 1$ are odd primes show that $(p/q) = (-1/p)$.

4 Show that $4^n \equiv 4 \pmod{12}$ for all integers $n \geq 1$. Use this result and Theorem 4.4 to show that 3 is a quadratic non-residue of each of the primes given in parts (a), (b) and (c) of Additional Exercise 2 of Section 3 above.

5 For which odd primes $p \neq 7$ does $(7/p) = 1$?

6 If p and q are distinct odd primes prove that $(-p/q) = (-q/p)$ if, and only if, $p \equiv q \equiv 1 \pmod{4}$.

Challenge Problems

1 Show that the product of the quadratic residues of an odd prime p is congruent modulo p to -1 when p is of the form $4k + 1$ and to 1 when p is of the form $4k + 3$.

2 Prove that there are infinitely many primes of the form $5k + 4$.

3 For any prime $p > 5$, prove that there are two consecutive integers which are both quadratic residues of p and two consecutive integers which are both quadratic non-residues of p.

4 Evaluate, for p an odd prime,

$$(1 \times 2/p) + (2 \times 3/p) + \cdots + ((p-2) \times (p-1)/p).$$

SOLUTIONS TO THE PROBLEMS

Solution 1.1

(a) Multiplying through by 20:

$$100x^2 + 140x + 20 \equiv 0 \pmod{13},$$

and completing the square:

$$(10x + 7)^2 - 29 \equiv 0 \pmod{13}.$$

That is,

$$(10x + 7)^2 \equiv 29 \equiv 16 \pmod{13}.$$

As $16 = (\pm 4)^2$, the required solutions are obtained by solving $10x + 7 \equiv \pm 4 \pmod{13}$. These are

$$x \equiv 1 \pmod{13} \quad \text{and} \quad x \equiv 8 \pmod{13}.$$

(b) Multiplying through by 4:

$$4x^2 + 4x + 4 \equiv 0 \pmod 5\,,$$

and completing the square:

$$(2x + 1)^2 + 3 \equiv 0 \pmod 5\,.$$

Adding 2 to both sides gives

$$(2x + 1)^2 \equiv 2 \pmod 5\,.$$

But the squares modulo 5 are 0, 1 and 4, and so the congruence

$$y^2 \equiv 2 \pmod 5\,,$$

has no solutions, and therefore the original congruence in x has no solutions.

(c) Multiplying through by 4 and completing the square:

$$(2x + 3)^2 + 7 \equiv 0 \pmod 7\,.$$

That is,

$$(2x + 3)^2 \equiv 0 \pmod 7\,.$$

So this has a unique solution which satisfies

$$2x + 3 \equiv 0 \pmod 7\,,$$

namely $x \equiv 2 \pmod 7$.

Solution 1.2

Working modulo 13:

$$1^2 \equiv 12^2 \equiv 1; \quad 2^2 \equiv 11^2 \equiv 4; \quad 3^2 \equiv 10^2 \equiv 9;$$
$$4^2 \equiv 9^2 \equiv 3; \quad 5^2 \equiv 8^2 \equiv 12; \quad 6^2 \equiv 7^2 \equiv 10.$$

The quadratic residues of 13 are therefore 1, 3, 4, 9, 10 and 12, and the non-residues, 2, 5, 6, 7, 8 and 11.

The congruence $x^2 + x - c \equiv 0 \pmod{13}$ has two solutions when its discriminant, $1 + 4c$, is a quadratic residue of 13, and has a unique solution when the discriminant is congruent to 0.

$$\begin{aligned}
1 + 4c &\equiv 0 \pmod{13} &&\iff c \equiv 3 \pmod{13}\\
1 + 4c &\equiv 1 \pmod{13} &&\iff c \equiv 0 \pmod{13}\\
1 + 4c &\equiv 3 \pmod{13} &&\iff c \equiv 7 \pmod{13}\\
1 + 4c &\equiv 4 \pmod{13} &&\iff c \equiv 4 \pmod{13}\\
1 + 4c &\equiv 9 \pmod{13} &&\iff c \equiv 2 \pmod{13}\\
1 + 4c &\equiv 10 \pmod{13} &&\iff c \equiv 12 \pmod{13}\\
1 + 4c &\equiv 12 \pmod{13} &&\iff c \equiv 6 \pmod{13}
\end{aligned}$$

So the congruence has solutions when $c \equiv 0, 2, 3, 4, 6, 7$ or $12 \pmod{13}$.

Solution 1.3

According to Euler's Criterion, 5 is a quadratic residue of prime p if, and only if, $5^{(p-1)/2} \equiv 1 \pmod p$.

$$5^{(11-1)/2} = 5^5 \equiv 25 \times 25 \times 5 \equiv 3 \times 3 \times 5 \equiv 45 \equiv 1 \pmod{11}$$
$$5^{(17-1)/2} = 5^8 \equiv (5^2)^4 \equiv 8^4 \equiv 64^2 \equiv (-4)^2 \equiv -1 \pmod{17}$$
$$5^{(19-1)/2} = 5^9 \equiv 5 \times (5^2)^4 \equiv 5 \times 6^4 \equiv 5 \times (-2)^2 \equiv 1 \pmod{19}$$

So 5 is a quadratic residue of 11 and 19 but is a quadratic non-residue of 17.

Solution 1.4

(a) Since, being a square, x^2 is a quadratic residue of p, the table informs us that a and b must be of the same quadratic character. That is, a is a quadratic residue of p if, and only if, b is a quadratic residue of p.

(b) If -1 is a quadratic residue of p then, according to Euler's Criterion, $(-1)^{(p-1)/2} = 1$ and so $\dfrac{p-1}{2}$ is an even integer. That is, $p \equiv 1 \pmod 4$.

(c) Since $p - a \equiv -a \equiv (-1)a \pmod p$, a and $p - a$ will be of the same quadratic character when -1 is a quadratic residue of p. Hence $p - a$ will also be a quadratic residue precisely when $p \equiv 1 \pmod 4$.

Solution 2.1

$$\begin{aligned}
(30/11) &= (8/11), && \text{by property (a)},\\
&= (2/11)(4/11), && \text{by property (c)},\\
&= (2/11), && \text{by property (b)},\\
&= (-9/11), && \text{by property (a)},\\
&= (-1/11)(9/11), && \text{by property (c)},\\
&= (-1/11), && \text{by property (b)},\\
&= -1, && \text{by property (e)}.
\end{aligned}$$

Alternatively by property (d).

Solution 2.2

(a)
$$\begin{aligned}
(3/11) &= (3/11)(2^2/11), && \text{since } (2^2/11) = 1 \text{ by property (b)},\\
&= (3 \times 2^2/11), && \text{by property (c)},\\
&= (12/11)\\
&= (1/11), && \text{by property (a)},\\
&= 1, && \text{by property (b)}.
\end{aligned}$$

(b)
$$\begin{aligned}
(2/17) &= (36/17), && \text{by property (a)},\\
&= 1, && \text{by property (b), since } 36 = 6^2.
\end{aligned}$$

(c)
$$\begin{aligned}
(40/11) &= (10/11)(4/11), && \text{by property (c)},\\
&= (10/11), && \text{by property (b)},\\
&= (-1/11), && \text{by property (a)},\\
&= -1, && \text{by property (e)}.
\end{aligned}$$

Solution 2.3

For the first part, the essential task is to show that $(2/31) = 1$. There are various ways of achieving this, such as to appeal to Euler's Criterion and show that $2^{15} \equiv 1 \pmod{31}$. Simpler, if you spot it, is to capitalize on the observation that $2 \equiv 64 \pmod{31}$ and so $(2/31) = (64/31) = 1$, since $64 = 8^2$. Then

Alternatively using property (d) of Theorem 2.1.

$$(2a/31) = (2/31)(a/31) = (a/31),$$

as required.

To make use of this result, take any quadratic residue of 31 and repeatedly double, finding further quadratic residues. For example, starting from 1:

$$1,\ 2,\ 4,\ 8, \text{ and } 16 \text{ are quadratic residues.}$$

Starting from $9 = 3^2$ we have further quadratic residues:

$$9,\ 18,\ 36 \equiv 5,\ 10, \text{ and } 20.$$

Starting from $25 = 5^2$ completes the list:

$$25,\ 50 \equiv 19,\ 38 \equiv 7,\ 14 \text{ and } 28.$$

As 31 is known to have fifteen quadratic residues, we have found them all:

$$1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25 \text{ and } 28.$$

Solution 3.1

(a) To evaluate $(7/13)$ we first form the set S consisting of the first $\frac{13-1}{2} = 6$ multiples of 7:

$$S = \{7, 14, 21, 28, 35, 42\},$$

and convert to S' by replacing each integer by its least positive residue modulo 13:

$$S' = \{\underline{7}, 1, \underline{8}, 2, \underline{9}, 3\}.$$

It is quite possible to go direct to the set S', by-passing S, by starting with 7 and writing down six integers getting from one to the next by adding 7 modulo 13.

The three underlined members exceed $\frac{13}{2}$ and so

$$(7/13) = (-1)^3 = -1.$$

(b) Repeating for $(11/23)$:

$$S = \{11, 22, 33, 44, 55, 66, 77, 88, 99, 110, 121\};$$

$$S' = \{11, \underline{22}, 10, \underline{21}, 9, \underline{20}, 8, \underline{19}, 7, \underline{18}, 6\}.$$

The five underlined members of S' exceed $\frac{23}{2}$ and so

$$(11/23) = (-1)^5 = -1.$$

(c) Finally for $(5/29)$, the first fourteen positive multiples of 5 give, modulo 29, the set

$$S' = \{5, 10, \underline{15}, \underline{20}, \underline{25}, 1, 6, 11, \underline{16}, \underline{21}, \underline{26}, 2, 7, 12\},$$

which has the six underlined members exceeding $\frac{29}{2}$, and so

$$(5/29) = (-1)^6 = 1.$$

Solution 3.2

(a) $(2/29) = -1$, since $29 \equiv 5 \pmod 8$.

(b) $(2/31) = 1$, since $31 \equiv 7 \pmod 8$.

(c) $(2/43) = -1$, since $43 \equiv 3 \pmod 8$.

Solution 3.3

By Gauss' Lemma, $(-2/p) = (-1)^n$, where n is the number of integers in the set $S = \{-2, -4, -6, \ldots, -2k, \ldots, -(p-1)\}$ which have least positive residue exceeding $\frac{p}{2}$. The least positive residue modulo p of each of the integers in S is obtained by adding p, giving

$$S' = \{1, 3, \ldots, p-2k, \ldots, p-4, p-2\}.$$

Now $p - 2k > \frac{p}{2}$ if, and only if, $k < \frac{p}{4}$, and therefore $n = \operatorname{int}\left(\frac{p}{4}\right)$. Looking at the four possible congruence classes of p modulo 8:

$$p = 8k+1 \implies n = \operatorname{int}\left(2k + \tfrac{1}{4}\right) = 2k;$$

$$p = 8k+3 \implies n = \operatorname{int}\left(2k + \tfrac{3}{4}\right) = 2k;$$

$$p = 8k+5 \implies n = \operatorname{int}\left(2k + \tfrac{5}{4}\right) = 2k+1;$$

$$p = 8k+7 \implies n = \operatorname{int}\left(2k + \tfrac{7}{4}\right) = 2k+1.$$

Now when n is even $(-2/p) = 1$, and this occurs when $p \equiv 1$ or $3 \pmod 8$. When n is odd $(-2/p) = -1$, and this occurs when $p \equiv 5$ or $7 \pmod 8$.

Solution 3.4

To make use of $(-2/p) = (-1/p)(2/p)$ we look at the four cases for p modulo 8, and multiply the value of $(-1/p)$, obtained from property (e) of Theorem 2.1, by the value of $(2/p)$, obtained from from Theorem 3.2.

$p \equiv 1 \pmod 8 \implies (-1/p) = 1$ and $(2/p) = 1$, so $(-2/p) = 1$
$p \equiv 3 \pmod 8 \implies (-1/p) = -1$ and $(2/p) = -1$, so $(-2/p) = 1$
$p \equiv 5 \pmod 8 \implies (-1/p) = 1$ and $(2/p) = -1$, so $(-2/p) = -1$
$p \equiv 7 \pmod 8 \implies (-1/p) = -1$ and $(2/p) = 1$, so $(-2/p) = -1$

This agrees with the result of Problem 3.3.

Solution 3.5

Suppose that $p_1, p_2, \ldots, p_n$ are the only primes of form $8k+3$, and let $N = (p_1p_2\ldots p_n)^2 + 2$. Since, for each $1 \le i \le n$, $p_i^2 \equiv 1 \pmod 8$, we note that $N \equiv 3 \pmod 8$. Now if p is any prime divisor of the odd integer N we have $(p_1p_2\ldots p_n)^2 \equiv -2 \pmod p$ and so, as the left-hand side is a square, $(-2/p) = 1$. The result of Problem 3.3 confirms that p is congruent modulo 8 either to 1 or to 3.

We have seen that the square of any odd integer, prime or composite, is congruent modulo 8 to 1.

At this point we can invoke the argument seen in the proof of Theorem 3.5. If all the prime divisors of N are congruent modulo 8 to 1 then so too is N itself. But N is not congruent modulo 8 to 1 and so it must have at least one prime divisor, say q, which is congruent modulo 8 to 3. This means that q must be one of the listed primes p_i. But then, q divides N and q divides $(p_1p_2\ldots p_n)^2$ which leads to the contradiction that q divides 2.

Hence there are infinitely many primes of the form $8k+3$.

Solution 4.1

(a) There are many possible sequences of steps, of which this is one. We have given an explanation of each step rather than a reference to the result being used.

$$\begin{aligned}
(-219/383) &= (-1/383)(3/383)(73/383), \quad \text{since } -219 = (-1)\times 3\times 73,\\
&= (-1)(3/383)(73/383), \quad \text{since } 383 \equiv 3 \pmod 4,\\
&= (-1)(-1)(383/3)(73/383), \quad \text{by LQR since } 383 \equiv 3 \pmod 4,\\
&= (2/3)(73/383), \quad \text{since } 383 \equiv 2 \pmod 3,\\
&= (-1)(73/383), \quad \text{since } 3 \equiv 3 \pmod 8,\\
&= (-1)(383/73), \quad \text{by LQR since } 73 \equiv 1 \pmod 4,\\
&= (-1)(18/73), \quad \text{since } 383 \equiv 18 \pmod{73},\\
&= (-1)(2/73)(9/73), \quad \text{since } 18 = 2\times 9,\\
&= (-1)(1)(9/73), \quad \text{since } 73 \equiv 1 \pmod 8,\\
&= (-1)(1)(1), \quad \text{since } 9 = 3^2,\\
&= -1.
\end{aligned}$$

We have consistently adopted the 'invert and divide' approach in this solution; but there are other methods. For example, the observation that $-219 \equiv 164 \pmod{383}$ and $164 = 4 \times 41$ offers

$$(-219/383) = (4/383)(41/383) = (41/383) = \ldots$$

as an alternative start.

(b) Whereas we spelled out each step in part (a), here we shall reduce the number of steps by processing several symbols simultaneously.

$$\begin{aligned}
(461/773) &= (773/461), \quad \text{by LQR},\\
&= (312/461), \quad \text{since } 773 \equiv 312 \pmod{461},\\
&= (4/461)(2/461)(3/461)(13/461), \quad \text{since } 312 = 2^3 \times 3 \times 13,\\
&= (1)(-1)(461/3)(461/13), \quad \text{since } 461 \equiv 5 \pmod 8 \text{ and by LQR twice},\\
&= (-1)(2/3)(6/13), \quad \text{since } 461 \equiv 2 \pmod 3 \text{ and } 461 \equiv 6 \pmod{13},\\
&= (-1)(-1)(2/13)(3/13), \quad \text{since } (2/3) = -1 \text{ and } 6 = 2 \times 3,\\
&= (-1)(13/3), \quad \text{since } 13 \equiv 5 \pmod 8 \text{ and by LQR},\\
&= (-1)(1/3), \quad \text{since } 13 \equiv 1 \pmod 3,\\
&= -1.
\end{aligned}$$

Solution 4.2

$$\begin{aligned}
(164/197) &= (4/197)(41/197), \quad \text{since } 164 = 4 \times 41,\\
&= (41/197), \quad \text{since 4 is a square},\\
&= (197/41), \quad \text{by LQR},\\
&= (74/41), \quad \text{since } 197 \equiv 74 \pmod{41},\\
&= (2/41)(37/41), \quad \text{since } 74 = 2 \times 37,\\
&= (37/41), \quad \text{since } 41 \equiv 1 \pmod 8,\\
&= (41/37), \quad \text{by LQR},\\
&= (4/37), \quad \text{since } 41 \equiv 4 \pmod{37},\\
&= 1, \quad \text{since 4 is a square.}
\end{aligned}$$

Solution 4.3

There are three major mistakes in the argument.

1. The step which replaces $(-19/79)$ by $(-1)(19/79)$ turns out to be correct but is handling the minus sign incorrectly. It should read $(-19/79) = (-1/79)(19/79)$. However, it happens that $(-1/79) = -1$, since $79 \equiv 3 \pmod 4$, so the misuse has not resulted in a wrong value being carried forward.
2. The first application of LQR is wrong. As $19 \equiv 79 \equiv 3 \pmod 4$, LQR gives $(19/79) = (-1)(79/19)$.
3. The second application of LQR is also wrong. As 15 is not a prime, LQR cannot be applied to Legendre symbol $(15/19)$. The correct continuation here would be $(15/19) = (3/19)(5/19)$. This mistake is compounded in the next line too, where the symbol $(19/15)$ is manipulated. As 15 is not prime this is not a legitimate Legendre symbol.

Solution 4.4

(a) The quadratic congruence $3x^2 + 6x + 5 \equiv 0 \pmod{89}$ is solvable provided $6^2 - 4 \times 3 \times 5 = -24$ is a quadratic residue of the prime 89.

$$\begin{aligned}
(-24/89) &= (65/89)\\
&= (5/89)(13/89)\\
&= (89/5)(89/13)\\
&= (4/5)(11/13)\\
&= (1)(13/11)\\
&= (2/11)\\
&= -1.
\end{aligned}$$

The congruence has no solutions.

(b) The quadratic congruence $2x^2 + 5x - 9 \equiv 0 \pmod{11 \times 101}$ has solutions if, and only if, each of the congruences $2x^2 + 5x - 9 \equiv 0 \pmod{11}$ and $2x^2 + 5x - 9 \equiv 0 \pmod{101}$ are solvable. This will be the case if $5^2 - 4 \times 2 \times (-9) = 97$ is a quadratic residue of both 11 and 101.

See Section 4.3 of *Unit 4*.

$$(97/11) = (9/11) = (3^2/11) = 1$$
$$(97/101) = (101/97) = (4/97) = (2^2/97) = 1$$

Note that 97 and 101 are primes.

Hence the congruence does have solutions.

Solution 4.5

We make use of the property $(6/p) = (2/p)(3/p)$ and the established facts

$(2/p) = 1$ if, and only if, $p \equiv \pm 1 \pmod 8$;
$(3/p) = 1$ if, and only if, $p \equiv \pm 1 \pmod{12}$.

To cater for modulo 8 and modulo 12 we shall need to consider the possible values of p modulo 24, which (since $p > 3$) are 1, 5, 7, 11, 13, 17, 19 and 23.

$\operatorname{lcm}(8, 12) = 24$

$p \equiv 1 \pmod{24} \implies (2/p) = 1$ and $(3/p) = 1$, so $(6/p) = 1$
$p \equiv 5 \pmod{24} \implies (2/p) = -1$ and $(3/p) = -1$, so $(6/p) = 1$
$p \equiv 7 \pmod{24} \implies (2/p) = 1$ and $(3/p) = -1$, so $(6/p) = -1$
$p \equiv 11 \pmod{24} \implies (2/p) = -1$ and $(3/p) = 1$, so $(6/p) = -1$
$p \equiv 13 \pmod{24} \implies (2/p) = -1$ and $(3/p) = 1$, so $(6/p) = -1$
$p \equiv 17 \pmod{24} \implies (2/p) = 1$ and $(3/p) = -1$, so $(6/p) = -1$
$p \equiv 19 \pmod{24} \implies (2/p) = -1$ and $(3/p) = -1$, so $(6/p) = 1$
$p \equiv 23 \pmod{24} \implies (2/p) = 1$ and $(3/p) = 1$, so $(6/p) = 1$

So $(6/p) = 1$ when $p \equiv 1, 5, 19$ or $23 \pmod{24}$.

Solution 4.6

We shall use the property $(-3/p) = (-1/p)(3/p)$ and the established facts

$(-1/p) = 1$ if, and only if, $p \equiv 1 \pmod 4$;
$(3/p) = 1$ if, and only if, $p \equiv \pm 1 \pmod{12}$.

We need to consider possible values of p modulo 12 which, since $p > 3$, are 1, 5, 7 and 11.

$p \equiv 1 \pmod{12} \implies (-1/p) = 1$ and $(3/p) = 1$, so $(-3/p) = 1$
$p \equiv 5 \pmod{12} \implies (-1/p) = 1$ and $(3/p) = -1$, so $(-3/p) = -1$
$p \equiv 7 \pmod{12} \implies (-1/p) = -1$ and $(3/p) = -1$, so $(-3/p) = 1$
$p \equiv 11 \pmod{12} \implies (-1/p) = -1$ and $(3/p) = 1$, so $(-3/p) = -1$

So $(-3/p) = 1$ when $p \equiv 1$ or $7 \pmod{12}$ and $(-3/p) = -1$ when $p \equiv 5$ or $11 \pmod{12}$.That is,

$$(-3/p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 6, \\ -1, & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

as claimed.

Now suppose that $p_1, p_2, \ldots, p_n$ are the only primes of the form $6k + 1$. Consider $N = (2p_1p_2 \ldots p_n)^2 + 3$. As N is odd it has an odd prime divisor, say p. Then $(2p_1p_2 \ldots p_n)^2 \equiv -3 \pmod p$, from which $(-3/p) = 1$ and the first part of the question gives $p \equiv 1 \pmod 6$. It now follows that p is one of the listed primes and so p is a divisor of $(2p_1p_2 \ldots p_n)^2$, and therefore of $N - (2p_1p_2 \ldots p_n)^2$. That is, p divides 3, and so $p = 3$. This contradicts the fact that p is of the form $6k + 1$, and so the assumption made, that there are only finitely many primes of this form, must be false.

Therefore there are infinitely many primes of the form $6k + 1$.

SOLUTIONS TO ADDITIONAL EXERCISES

Section 1

1 (a) Multiplying through by 8 and completing the square, the congruence becomes

$$(4x+4)^2 - 8 \equiv 0 \pmod{7}, \text{ i.e. } (4x+4)^2 \equiv 1 \pmod{7}.$$

This has solutions satisfying $4x + 4 \equiv \pm 1 \pmod{7}$. That is, $x \equiv 1 \pmod{7}$ and $x \equiv 4 \pmod{7}$.

(b) Writing the congruence as $3x^2 + 12x - 3 \equiv 0 \pmod{11}$ we can begin by cancelling the factor 3 to reach the equivalent congruence $x^2 + 4x - 1 \equiv 0 \pmod{11}$. That is,

$$(x+2)^2 - 5 \equiv 0 \pmod{11}, \text{ i.e. } (x+2)^2 \equiv 5 \equiv 16 \pmod{11}.$$

Hence $x + 2 \equiv \pm 4 \pmod{11}$, which leads to $x \equiv 2 \pmod{11}$ and $x \equiv 5 \pmod{11}$.

You could, of course, begin by multiplying through by 12, but you should be on the look-out for short-cuts.

2 The quadratic congruence $2x^2 - 5x + c \equiv 0 \pmod{13}$ has discriminant $25 - 8c$ and so the congruence has solutions when this is either a quadratic residue of 13 or is congruent to 0 modulo 13. Now $25 - 8c \equiv 5c - 1 \pmod{13}$ and, referring to the list of quadratic residues of 13 established in Example 1.3, for solutions we require

$$5c - 1 \equiv 0,\ 1,\ 3,\ 4,\ 9,\ 10,\ 12 \pmod{13}.$$

These linear congruences have, respectively, solutions

$$c \equiv 8,\ 3,\ 6,\ 1,\ 2,\ 10,\ 0 \pmod{13}.$$

Hence the original quadratic congruence has solutions for these values of c.

Solving for the case $c = 1$,

$$\begin{aligned} 2x^2 - 5x + 1 \equiv 0 \pmod{13} &\iff 16x^2 - 40x + 8 \equiv 0 \pmod{13} \\ &\iff (4x-5)^2 - 17 \equiv 0 \pmod{13} \\ &\iff (4x-5)^2 \equiv 4 \pmod{13} \\ &\iff 4x - 5 \equiv \pm 2 \pmod{13}. \end{aligned}$$

These linear congruences, and hence the quadratic congruence, have solutions $x \equiv 4 \pmod{13}$ and $x \equiv 5 \pmod{13}$.

3 (a) $$\begin{aligned} 3^{(23-1)/2} &= 3^{11} = 27 \times 27 \times 27 \times 9 \\ &\equiv 4^3 \times 9 \equiv (-5) \times 9 \equiv -45 \equiv 1 \pmod{23}. \end{aligned}$$

So 3 is a quadratic residue of 23.

(b) $$\begin{aligned} (3^{(29-1)/2} &= 3^{14} = 27^4 \times 9 \equiv (-2)^4 \times 9 \\ &\equiv 4 \times 36 \equiv 28 \equiv -1 \pmod{29}. \end{aligned}$$

So 3 is a quadratic non-residue of 29.

4 Suppose that $n > 2$, $\gcd(a, n) = 1$ and $x^2 \equiv a \pmod{n}$. Then $\gcd(x^2, n) = 1$, from which it follows that $\gcd(x, n) = 1$, since any common divisor of x and n would necessarily divide x^2. Now

$$a^{\phi(n)/2} \equiv (x^2)^{\phi(n)/2} \equiv x^{\phi(n)} \equiv 1 \pmod{n}, \text{ by Euler's Theorem.}$$

A counter-example to the converse is provided by case $a = 3$ and $n = 8$:

$$a^{\phi(n)/2} = 3^{\phi(8)/2} = 3^{4/2} = 9 \equiv 1 \pmod{8}.$$

However the only squares modulo 8 are 0, 1 and 4, and so there is no solution for $x^2 \equiv 3 \pmod{8}$.

Section 2

1 (a) The discriminant is $8^2 - 4 \times 1 \times 4 = 48$, so our task is to determine the Legendre symbol $(48/13)$.

The properties are those of Theorem 2.1.

$$\begin{aligned}(48/13) &= (16/13)(3/13), \quad \text{by property (c)},\\ &= (3/13), \quad \text{by property (b)},\\ &= (16/13), \quad \text{by property (a)},\\ &= 1, \quad \text{by property (b)}.\end{aligned}$$

The observation that $(48/13) = (9/13)$, by property (a), suggests an equally good approach.

So the congruence has solutions.

(b) The discriminant is $7^2 - 4 \times 1 \times 9 = 13$, so our task is to determine the Legendre symbol $(13/23)$.

$$\begin{aligned}(13/23) &= (36/23), \quad \text{by property (a)},\\ &= 1, \quad \text{by property (b)}.\end{aligned}$$

So the congruence has solutions.

2 (a) $$\begin{aligned}(18/19) &= (-1/19), \quad \text{by property (a)},\\ &= -1, \quad \text{by property (e)}.\end{aligned}$$

(b) $$\begin{aligned}(45/19) &= (5/19)(9/19), \quad \text{by property (c)},\\ &= (5/19), \quad \text{by property (b)},\\ &= (5/19)(4/19), \quad \text{since } (4/19) = 1 \text{ by property (b)},\\ &= (20/19), \quad \text{by property (c)},\\ &= (1/19), \quad \text{by property (a)},\\ &= 1.\end{aligned}$$

(c) $$\begin{aligned}(2/19) &= (2/19)(9/19), \quad \text{since } (9/19) = 1 \text{ by property (b)},\\ &= (18/19), \quad \text{by property (c)},\\ &= -1, \quad \text{from part (a) above.}\end{aligned}$$

3 Since $29 \equiv 1 \pmod 4$, $(-1/29) = 1$ by property (e) of Theorem 2.1. It now follows that for any quadratic residue a,

$$(-a/29) = (-1/29)(a/29) = 1 \times 1 = 1,$$

and so $-a$ is also a quadratic residue. In particular, as the 'squares' 1, 4, 9 and 16 are quadratic residues so too are $-1 \equiv 28$, $-4 \equiv 25$, $-9 \equiv 20$ and $-16 \equiv 13$.

The prime 29 has fourteen quadratic residues and so we seek a further six. Using the fact that 20 is a quadratic residue we have

$$1 = (20/29) = (4/29)(5/29) = (5/29),$$

so 5, and hence $-5 \equiv 24$, are quadratic residues. Similarly

$$1 = (28/29) = (4/29)(7/29) = (7/29),$$

There are other ways, such as using larger squares, of finding the remaining quadratic residues.

so that 7 and 22 are quadratic residues. Finally

$$1 = (5/29)(7/29) = (35/29) = (6/29),$$

giving 6 and 23 as the missing pair.

Collecting everything together the quadratic residues of 29 are

$$1,\ 4,\ 5,\ 6,\ 7,\ 9,\ 13,\ 16,\ 20,\ 22,\ 23,\ 24,\ 25 \text{ and } 28.$$

4 By property (d) of Theorem 2.1

$$(a/p) \equiv a^{(p-1)/2} \pmod{p}$$

and therefore

$$(a/p)a^{(p-1)/2} \equiv (a/p)(a/p) \equiv 1 \pmod{p}\,.$$

Now Wilson's Theorem gives $(p-1)! \equiv -1 \pmod{p}$, and combining the two congruences we have

$$(p-1)! \equiv -(a/p)a^{(p-1)/2} \pmod{p}\,.$$

Section 3

1 (a) The set S comprises the first $\dfrac{13-1}{2}$ multiples of -3, thus

$$S = \{-3, -6, -9, -12, -15, -18\};$$

and replacing each integer by its least positive residue modulo 13,

$$S' = \{\underline{10}, \underline{7}, 4, 1, \underline{11}, \underline{8}\}.$$

The four underlined members have least positive residue exceeding $\dfrac{13}{2}$ and so $(-3/13) = (-1)^4 = 1$.

(b) Repeating for $(5/17)$:

$$S' = \{5, \underline{10}, \underline{15}, 3, 8, \underline{13}, 1, 6\}.$$

Three members of S' exceed $\dfrac{17}{2}$ and so $(5/17) = (-1)^3 = -1$.

We have gone directly to S' by starting with 5 and moving from one number to the next by adding 5 modulo 17 until we have eight numbers.

2 Using Theorem 3.2, which tells us that 2 is a quadratic residue of p if, and only if, $p \equiv \pm 1 \pmod{8}$, we aim to determine the value of each of the given primes modulo 8.

(a) For $n > 1$, 8 divides 4^n and so $4^n + 1 \equiv 1 \pmod{8}$.

(b) For $p \geq 3$, 8 divides 2^p and so $2^p - 1 \equiv -1 \pmod{8}$. However, for $p = 2$, $M_2 = 3$ and hence 2 is not a quadratic residue of M_2.

(c) For $n > 1$, 8 divides 2^{2^n} and so $2^{2^n} + 1 \equiv 1 \pmod{8}$.

In all cases 2 is a quadratic residue of the given prime.

From $(-2/p) = (2/p)(-1/p)$ it follows that -2 will be a quadratic residue provided -1 is a quadratic residue, and this we know, from property (e) of Theorem 2.1, will occur exactly when $p \equiv 1 \pmod{4}$. Hence we have the following results.

(a) $4^n + 1 \equiv 1 \pmod{4}$, so -2 is a quadratic residue.

(b) For $p > 2$, $2^p - 1 \equiv -1 \pmod{4}$, so -2 is a quadratic non-residue.

(c) $2^{2^n} + 1 \equiv 1 \pmod{4}$, so -2 is a quadratic residue.

Notice that -2 is a quadratic residue of $M_2 = 3$.

3 Suppose that $p_1, p_2, \ldots, p_n$ are the only primes of form $8k+5$. Consider the integer $N = 4(p_1p_2\ldots p_n)^2 + 1$. We observe that as each $p_i^2 \equiv 25 \equiv 1 \pmod 8$, N itself is of the form $8k+5$. Being odd, N has some odd prime divisor p, and the congruence

$$4(p_1p_2\ldots p_n)^2 \equiv -1 \pmod p$$

leads to $(-1/p) = 1$, as the left-hand side is a square. Property (e) of Theorem 2.1 now gives $p \equiv 1 \pmod 4$; that is, $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$.

The rest of the argument should be familiar. If all the prime divisors of N are of the form $8k+1$ then so too would be N itself. This is not the case and hence N must have at least one prime divisor of the form $8k+5$; that is, N is divisible by one of the primes p_i. But then p_i divides $N - 4(p_1p_2\ldots p_n)^2 = 1$, which is the required contradiction.

Hence there are infinitely many primes of the form $8k+5$.

Section 4

The properties are those of Theorem 2.1.

1 (a) $(35/71) = (5/71)(7/71)$, by property (c),
$= (71/5)(-1)(71/7)$, by LQR, noting $7 \equiv 71 \equiv 3 \pmod 4$,
$= (1/5)(-1)(1/7)$, by property (a),
$= -1$.

(b) $(139/149) = (149/139)$, by LQR, both integers are prime and $149 \equiv 1 \pmod 4$,
$= (10/139)$, by property (a),
$= (2/139)(5/139)$, by property (c),
$= (-1)(139/5)$, by Theorem 3.2 and LQR respectively,
$= (-1)(4/5)$, by property (a),
$= -1$, by property (b).

(c) $(1234/4567) = (2/4567)(617/4567)$, by property (c),
$= (1)(4567/617)$, by Theorem 3.2 and LQR, noting that 617 is prime and $617 \equiv 1 \pmod 4$,
$= (248/617)$, by property (a) since $7 \times 617 = 4319$,
$= (4/617)(2/617)(31/617)$, by property (c),
$= (1)(1)(617/31)$, by Theorem 3.2 and LQR,
$= (28/31)$, by property (a),
$= (4/31)(7/31)$, by property (c),
$= (1)(-1)(31/7)$, by property (b) and LQR,
$= (-1)(3/7)$, by property (a),
$= (-1)(-1)(7/3)$, by LQR,
$= (1/3)$, by property (a),
$= 1$.

2 (a) The discriminant is $1^2 - 4 \times 3 \times (-7) = 85 \equiv 0 \pmod{17}$, so the congruence has a unique solution.

(b) The discriminant is $1^2 - 4 \times 2 \times 1 = -7$, so the existence or otherwise of solutions is determined by the value of $(-7/29)$.

$(-7/29) = (-1/29)(7/29)$, by property (c),
$= (1)(29/7)$, by property (e) and LQR,
$= (1/7) = 1$.

The congruence has solutions.

(c) The discriminant is $3^2 - 4 \times 2 \times (-7) = 65$, so we investigate $(65/101)$.

$$\begin{aligned}(65/101) &= (5/101)(13/101)\\ &= (101/5)(101/13)\\ &= (1/5)(10/13)\\ &= (1)(10/13)\\ &= (40/13), \quad \text{by property (c), using } (4/13) = 1,\\ &= (1/13) = 1.\end{aligned}$$

The congruence has solutions.

3 (a) If $p = 4k + 3$ then

$$q = 10p + 3 = 40k + 33 = 4(10k + 8) + 1 = 4k' + 1.$$

From this we see that p and q cannot both be congruent modulo 4 to 3. Hence LQR gives

$$(p/q) = (q/p) = (10p + 3/p) = (3/p).$$

Note that $10p + 3 \equiv 3 \pmod{p}$.

(b) We consider separately the possible values of p modulo 4.

If $p = 4k + 1$ then

$$(-1/p) = 1 \text{ and } (p/q) = (q/p) = (10p + 1/p) = (1/p) = 1.$$

If $p = 4k + 3$ then

$$(-1/p) = -1 \text{ and } q = 10p + 1 = 4(10k + 7) + 3,$$

and so

$$(p/q) = (-1)(q/p) = (-1)(10p + 1/p) = (-1)(1/p) = -1.$$

In both cases $(p/q) = (-1/p)$.

4 The fact that $4^n \equiv 4 \pmod{12}$ for all $n \geq 1$, is readily proved by Mathematical Induction. It is certainly true for $n = 1$ and the assumption that $4^k \equiv 4 \pmod{12}$ leads to

$$4^{k+1} = 4^k \times 4 \equiv 4 \times 4 \equiv 4 \pmod{12}.$$

Using this we obtain the following.

(a) $4^n + 1 \equiv 5 \pmod{12}$, for all $n \geq 1$.

(b) $2^p - 1 = 2 \times 4^{(p-1)/2} - 1 \equiv 2 \times 4 - 1 \equiv 7 \pmod{12}$, for all $p \geq 3$.

(c) $2^{2^n} + 1 \equiv 4^{2^{n-1}} + 1 \equiv 5 \pmod{12}$, for all $n \geq 1$.

By Theorem 4.4, the integer 3 is a quadratic non-residue of each of these primes.

5 For odd prime $p \neq 7$ we have:

$$(7/p) = \begin{cases} (p/7), & \text{if } p \equiv 1 \pmod{4},\\ (-1)(p/7), & \text{if } p \equiv 3 \pmod{4}.\end{cases}$$

The quadratic residues of 7 are 1, 2 and 4, so:

$1^2 = 1,\ 2^2 = 4,\ 3^2 \equiv 2 \pmod{7}$

$$(p/7) = \begin{cases} 1, & \text{if } p \equiv 1, 2 \text{ or } 4 \pmod{7},\\ -1, & \text{if } p \equiv 3, 5 \text{ or } 6 \pmod{7}.\end{cases}$$

Putting the two parts together, $(7/p) = 1$ if, and only if,

$$\begin{aligned}&\text{either} \quad p \equiv 1 \pmod{4} \quad \text{and} \quad p \equiv 1, 2 \text{ or } 4 \pmod{7},\\ &\text{or} \quad p \equiv 3 \pmod{4} \quad \text{and} \quad p \equiv 3, 5 \text{ or } 6 \pmod{7}.\end{aligned}$$

That is,

$$(7/p) = 1 \text{ if, and only if, } p \equiv 1, 3, 9, 19, 25 \text{ or } 27 \pmod{28}.$$

6 Consider first the case $p \equiv q \equiv 3 \pmod 4$. Then

$$(-p/q) = (-1/q)(p/q) = (-1)(p/q) = (-1)(-1)(q/p) = (q/p)$$

while

$$(-q/p) = (-1/p)(q/p) = (-1)(q/p),$$

and so $(-p/q) \neq (-q/p)$.

In all other cases

$$(-p/q) = (-1/q)(p/q) = (-1/q)(q/p),$$

while

$$(-q/p) = (-1/p)(q/p),$$

and the two will be equal when $(-1/q) = (-1/p)$. This happens when $p \equiv q \pmod 4$. As the case $p \equiv q \equiv 3 \pmod 4$ has been eliminated, we conclude that

$$(-p/q) = (-q/p) \text{ if, and only if, } p \equiv q \equiv 1 \pmod 4\,.$$

INDEX

$(-1/p)$ 12
$(-2/p)$ 19
$(2/p)$ 18
$(3/p)$ 27
(a/p) 12
int(x) 18

discriminant 5

Euler's Criterion 7

Gauss' Lemma 15

Jacobi symbol 28

Law of Quadratic Reciprocity 21
Legendre symbol, (a/p) 12
LQR 21
LQR an alternative formulation 21

primitive root 10

quadratic character 5
quadratic character of 2, $(2/p)$ 18
quadratic character of 3, $(3/p)$ 27
quadratic congruence 4
quadratic non-residue 5
quadratic residue 5